Analysis

$(fg)' = f'g + fg'$

$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$

$(f(g))' = f'(g)g'$

$(\sin(x))' = \cos(x)$

$(\cos(x))' = -\sin(x)$

$(\tan(x))' = \sec^2(x)$

$(\cot(x))' = -\csc^2(x)$

$(\sec(x))' = \sec(x)\tan(x)$

$(\csc(x))' = -\csc(x)\cot(x)$

$(e^x)' = e^x$

$(a^x)' = a^x \ln(a)$

$(\ln(x))' = \frac{1}{x}$

$(\ln(f(x)))' = \frac{f'(x)}{f(x)}$

$(\arcsin(x))' = \frac{1}{\sqrt{1-x^2}}$

$(\arctan(x))' = \frac{1}{1+x^2}$

$(\operatorname{arcsec}(x))' = \frac{1}{|x|\sqrt{x^2-1}}$

$\sin^2(a) + \cos^2(a) = 1$

$1 + \tan^2(a) = \sec^2(a)$

$1 + \cot^2(a) = \csc^2(a)$

$\sin(a+b) = \sin(a)\cos(b) + \sin(b)\cos(a)$

$\sin(2a) = 2\sin(a)\cos(a)$

$\sin(3a) = 3\sin(a) - 4\sin^3(a)$

$\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$

$\cos(2a) = \cos^2(a) - \sin^2(a) =$
$2\cos^2(a) - 1 = 1 - 2\sin^2(a)$

$\cos(3a) = 4\cos^3(a) - 3\cos(a)$

$\tan(a+b) = \frac{\tan(a)+\tan(b)}{1-\tan(a)\tan(b)}$

$\tan(2a) = \frac{2\tan(a)}{1-\tan^2(a)}$

$\tan(3a) = \frac{3\tan(a)-\tan^3(a)}{1-3\tan^2(a)}$

$\sin(a)\sin(b) = \frac{1}{2}(\cos(a-b) - \cos(a+b))$

$\cos(a)\cos(b) = \frac{1}{2}(\cos(a-b) + \cos(a+b))$

$\sin(a)\cos(b) = \frac{1}{2}(\sin(a+b) + \sin(a-b))$

$\cos(a)\sin(b) = \frac{1}{2}(\sin(a+b) - \sin(a-b))$

$\sin(a) + \sin(b) = 2\sin\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right)$

$\cos(a) + \cos(b) = 2\cos\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right)$

$\sin(a) = \frac{1}{2i}(e^{ia} - e^{-ia})$

$\cos(a) = \frac{1}{2}(e^{ia} + e^{-ia})$

$(a+ib)(c+id) = (ac-bd) + i(ad+bc)$
so $(a,b),(c,d) \to (ac-bd, ad+bc)$

$\int \frac{1}{x}dx = \ln(|x|)$

$\int e^x dx = e^x$

$\int a^x dx = \frac{a^x}{\ln(a)}$

$\int \ln(x)dx = x\ln(x) - x$

$\int \sin(x)dx = -\cos(x)$

$\int \cos(x)dx = \sin(x)$

$\int \tan(x)dx = -\ln|\cos(x)|$

$\int \cot(x)dx = \ln|\sin(x)|$

$\int \sec(x)dx = \ln|\sec(x)+\tan(x)|$

$\int \csc(x)dx = \ln|\csc(x)-\cot(x)|$

$\int \sec^2(x)dx = \tan(x)$

$\int \sec(x)\tan(x)dx = \sec(x)$

$\int \csc^2(x)dx = -\cot(x)$

$\int \csc(x)\cot(x)dx = -\csc(x)$

$\int \tan^2(x)dx = \tan(x) - x$

$\int \frac{1}{\sqrt{a^2-x^2}}dx = \arcsin\left(\frac{x}{a}\right)$

$\int \frac{1}{a^2+x^2}dx = \frac{1}{a}\arctan\left(\frac{x}{a}\right)$

$\int \frac{1}{x\sqrt{x^2-a^2}}dx = \frac{1}{a}\text{arcsec}\left(\frac{|x|}{a}\right)$

$[f^{-1}]'(a) = \frac{1}{f'(f^{-1}(a))}$

$\int_a^b f(x)dx + \int_{f(a)}^{f(b)} f^{-1}(x)dx =$
$bf(b) - af(a)$

u-Substitution: $\frac{du}{dx}$ and integral bounds.

Integration By Parts:
$uv = \int udv + \int vdu$, $u(x)v(x)|_a^b =$
$\int_a^b u(x)v'(x)dx + \int_a^b u'(x)v(x)dx$ i.e.
reducing degree of x^n or creating
system of equations in sin and cos

$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$

Mean Value: if f is continuous on $[a,b]$
and differentiable on (a,b) then there
exists $c \in (a,b)$ such that
$f'(c) = \frac{f(b)-f(a)}{b-a}$

L'Hospital: if $\lim_{x\to a}\frac{f(x)}{g(x)} = \frac{0}{0}$ or
$\lim_{x\to a}\frac{f(x)}{g(x)} = \frac{\pm\infty}{\pm\infty}$ then
$\lim_{x\to a}\frac{f(x)}{g(x)} = \lim_{x\to a}\frac{f'(x)}{g'(x)}$

Feynman-Leibniz: differentiate under
the integral e.g. to compute $\int_0^1 \frac{\ln(x+1)}{x^2+1}dx$
note $I(a) = \int_0^1 \frac{\ln(ax+1)}{x^2+1}dx$ has $I(0) = 0$
and $\frac{dI}{da} = \int_0^1 \frac{x}{(ax+1)(x^2+1)}dx$

Taylor Series: $\sum_{n=0}^{\infty}\frac{f^{(n)}(a)}{n!}(x-a)^n$

With Remainder: $f(x) =$
$\sum_{n=0}^{m-1}\frac{f^{(n)}(a)}{n!}(x-a)^n + \frac{f^{(m)}(c)}{m!}(x-a)^n$ for
some $c \in [x,a]$

$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots$

$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots$

$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots$

$\ln(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \ldots$

$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots$

$\arctan(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots$

Partial Fractional Decomposition

$(\ln(P(x)))' = \frac{P'(x)}{P(x)} =$
$\frac{1}{x-x_1} + \frac{1}{x-x_2} + \cdots + \frac{1}{x-x_n}$

Riemann Sums Trapezoids Rectangles
Dominating Inequalities

Implicit Differentiation

Squeeze: $a_n \le b_n \le c_n$ and a_n, c_n
converge to L so does b_n

Passing The Limit: e.g.
$x_{n+1} = 1 + \frac{1}{x_n} \to L = 1 + \frac{1}{L}$

Stirling: $n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdot e^{\frac{\theta_n}{12n}}$ for $0 < \theta_n < 1$, $\lim_{n\to\infty} \frac{n}{(n!)^{\frac{1}{n}}} = e$

Stolz-Cesaro: if b_n is strictly monotone and divergent or $\lim_{n\to\infty} a_n, b_n = 0$ and $\lim_{n\to\infty} \frac{a_{n+1}-a_n}{b_{n+1}-b_n} = l$ then $\lim_{n\to\infty} \frac{a_n}{b_n} = l$

Bolzano-Weierstrass: every bounded sequence in $\mathbb{R}^n$ has a convergent subsequence.

Monotone Convergence: a monotone bounded sequence converges to its extremum.

Harmonic Series: $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ diverges partial sum $\leq \ln(n) + 1$

$\sum \frac{1}{n\ln(n)}$ Diverges: $\int \frac{1}{x\ln(x)} = \ln(\ln(x))$

$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots$

$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$

Equidistribution Criterion: if f is a continuous periodic function with irrational period and $\sum \frac{|f(n)|}{n} < \infty$ then $f = 0$

Intermediate Value Property: if $f(x)$ is continuous on $[a, b]$ and $c \in (f(a), f(b))$ then there exists $d \in (a, b)$ such that $f(d) = c$

Ratio Test: convergence of series $\sum_{n=1}^{\infty} a_n$ from $L = \lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right|$
$L < 1$ then the series converges absolutely.
$L > 1$ then the series is divergent.
$L = 1$ or does not exist then inconclusive.

Root Test: convergence of series $\sum_{n=1}^{\infty} a_n$ from $L = \lim_{n\to\infty} |a_n|^{\frac{1}{n}}$
$L < 1$ then the series converges absolutely.
$L > 1$ then the series is divergent.
$L = 1$ or does not exist then inconclusive.

Alternating Series Test: if the series $\sum_{n=1}^{\infty} a_n$ is alternating (in sign), that is $a_n = (-1)^n b_n$ or $a_n = (-1)^{n+1} b_n$ where $b_n \geq 0$ then the series is convergent if:
$\lim_{n\to\infty} b_n = 0$ and
$\{b_n\}$ is a decreasing sequence.

Cauchy Condensation Test: for a monotone decreasing sequence $f(n) \geq 0$ of non negative real numbers, the series $\sum_{n=1}^{\infty} f(n)$ converges if and only if the condensed series $\sum_{n=0}^{\infty} 2^n f(2^n)$ converges. Moreover, if they converge, the sum of the condensed series is no more than twice as large as the sum of the original. Commonly useful when n appears in the denominator of the series. For the most basic example of this sort, the harmonic series $\sum \frac{1}{n}$ is transformed in to the series $\sum 1$ which diverges.

Borsuk-Ulam: any continuous map of the sphere in to $\mathbb{R}^2$ sends 2 antipodal points on the sphere to the same point in $\mathbb{R}^2$. A nice interpretation of this fact is that at any time there are 2 antipodal points on Earth with the same temperature and barometric pressure.

Lebesgue: there exists a function $f : [0, 1] \to [0, 1]$ that has the

intermediate value property and is discontinuous at every point.

Complex Analysis

Rotational

$V = \int y^2 \pi dx$

$S = \int 2\pi y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$

Vector Calculus

$ds = \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

$dS = \sqrt{1 + f_x^2 + f_y^2} dxdy$

Gradient Line Integrals:
$\int_C \nabla f \cdot ds = f(b) - f(a)$

Green: $\int_C F \cdot ds = \int_C F_1 dx + F_2 dy =$
$\int \int_D \left(\frac{dF_2}{dx} - \frac{dF_1}{dy}\right) dA$

Stoke: $\int_C F \cdot ds = \int \int_S \text{curl}(F) \cdot dS$

$$\text{curl}(F) = \nabla \times F = \begin{vmatrix} i & j & k \\ \frac{d}{dx} & \frac{d}{dy} & \frac{d}{dz} \\ F_1 & F_2 & F_3 \end{vmatrix} =$$
$\left(\frac{dF_3}{dy} - \frac{dF_2}{dz}\right) i + \left(\frac{dF_1}{dz} - \frac{dF_3}{dx}\right) j +$
$\left(\frac{dF_2}{dx} - \frac{dF_1}{dy}\right) k$

Divergence:
$\int \int_S F \cdot dS = \int \int \int_W \text{div}(F) dV$

$\text{div}(F) = \nabla \cdot F = \frac{dF_1}{dx} + \frac{dF_2}{dy} + \frac{dF_3}{dz}$

Change Of Variables: $\frac{d(x,y)}{d(a,b)} = \begin{vmatrix} \frac{dx}{da} & \frac{dx}{db} \\ \frac{dy}{da} & \frac{dy}{db} \end{vmatrix}$
whence $\int \int_R f(x,y) dA =$
$\int \int_S f(g(a,b), h(a,b)) \left|\frac{d(x,y)}{d(a,b)}\right| d\hat{A}$ and

similarly Jacobian for e.g. $\left|\frac{d(x,y,z)}{d(a,b,c)}\right|$

Rotational:
$x = r\cos(\theta), y = r\sin(\theta) \rightarrow \frac{d(x,y)}{d(r,\theta)} = r$
Cylindrical: $x = r\cos(\theta), y =$
$r\sin(\theta), z = z \rightarrow \frac{d(x,y,z)}{d(r,\theta,z)} = r$
Spherical: $x = r\sin(\phi)\cos(\theta), y =$
$r\sin(\phi)\sin(\theta), z = r\cos(\theta) \rightarrow \frac{d(x,y,z)}{d(r,\theta,\phi)} =$
$r^2 \sin(\phi)$

Surface Area

Ratio Of Area Projection Is $\cos(\theta)$

$\int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi}$

$\int_{-\infty}^{\infty} e^{-ax^2} dx = \sqrt{\frac{\pi}{a}}$

Fubini: Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ be a piecewise continuous function such that it is positive or $\int_c^d \int_a^b |f(x,y)| dxdy < \infty$.
Then
$\int_c^d \int_a^b f(x,y) dxdy = \int_a^b \int_c^d f(x,y) dydx$

Tonelli: if $\int_{X \times Y} |f(x,y)| d(x,y) < \infty$
then
$\int_{X \times Y} f(x,y) f d(x,y) =$
$\int_X \left(\int_Y f(x,y) dy\right) dx =$
$\int_Y \left(\int_X f(x,y) dx\right) dy$

Algebra

Smoothing

Vieta's: homogeneous expressions calculable from symmetric sums.

Polynomial Facts

If r is a real root of $P(x)$ with multiplicity > 1 then $P(r) = P'(r) = 0$

$(a-b)|(P(a)-P(b))$

Primitive:
$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ if
$\text{GCD}(a_n, a_{n-1} \ldots, a_1, a_0) = 1$

Gauss: if $P(x)$ and $Q(x)$ are primitive polynomials over the integers, then their product $P(x)Q(x)$ is also primitive.

Gauss: a non constant polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is both irreducible in $\mathbb{Q}[x]$ and primitive in $\mathbb{Z}[x]$

Suffices To Show $P(x+a)$ Irreducible

Eisenstein: let
$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and prime p such that:
$p|a_0, a_1, \ldots, a_{n-1}$
$p \nmid a_n$
$p^2 \nmid a_0$
Then $P(x)$ can not be expressed as the product of 2 non-constant polynomials with integer coefficients.

Perron: $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is irreducible if $a_0 \neq 0$ and
$|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$

Cohn: $b \geq 2$ and
$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ such that $0 \leq a_i \leq b-1$. If $p(b)$ is prime then $p(x)$ is irreducible.

Rational Root:
$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with integer coefficients with root $\frac{p}{q}$ then $p|a_0$ and $q|a_n$

Constructing Expressions From Plugging In To Polynomials

Lagrange Multipliers: $\nabla f = \lambda \nabla g$

Lagrange Interpolation: unique polynomial of degree at most n satisfying $P(x_i) = y_i$ for $n+1$ points is $\sum \left(P(x_i) \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \right)$

Finite Differences

Quadratic Formula: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Substitutions

Converting Between Algebra And Geometry

Perturbing The Particular Solution And Vieta Jumping

Identities

$a^2 - b^2 = (a+b)(a-b)$
$2021 = 47 \cdot 43$

$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$

$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$

$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)$

$a^4 + b^4 = (a^2 + \sqrt{2}ab + b^2)(a^2 - \sqrt{2}ab + b^2)$

$a^3+b^3+c^3-3abc =$
$(a+b+c)(a^2+b^2+c^2-ab-bc-ca) =$
$(a+b+c)(a+wb+w^2c)(a+w^2b+wc)$

$a^2+b^2+c^2-ab-bc-ca =$
$\frac{1}{2}((a-b)^2+(b-c)^2+(c-a)^2)$

$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2 =$
$(ac+bd)^2+(ad-bc)^2$

$1+2+3+\cdots+n = \frac{n(n+1)}{2}$
$1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, \ldots$

$1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$
$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$
$1, 5, 14, 30, 55, 91, 140, 204, 285, \ldots$

$1^3+2^3+3^3+\cdots+n^3 = \left(\frac{n(n+1)}{2}\right)^2$
$1, 8, 27, 64, 125, 216, 343, 512, 729, \ldots$
$1, 9, 36, 100, 225, 441, 784, 1296, \ldots$

$1^4+2^4+3^4+\cdots+n^4 =$
$\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$
$1, 16, 81, 256, 625, 1296, 2401, 4096, \ldots$
$1, 17, 98, 354, 979, 2275, 4676, 8772, \ldots$

Vieta-Newton-Girard:
$f(x) = x^n + s_1x^{n-1} + \cdots + s_{n-1}x + s_n$
Signed Symmetric Sums/Polynomials
$s_k = (-1)^k \sum_{j_1<\cdots<j_k} x_{j_1} \ldots x_{j_k}$
Power Sums/Polynomials
$p_k(x_1, \ldots, x_n) = x_1^k + \cdots + x_n^k$
$ks_k + \sum_{i=0}^{k-1} s_i p_{k-i} = 0$ if $k \leq n$
$\sum_{i=0}^{n} s_i p_{k-i} = 0$ if $k > n$

Logarithms

$\log_a b = c \iff a^c = b$

$\log_a b + \log_a c = \log_a bc$

$\log_a b^n = n \log_a b$

$\log_a b \cdot \log_b c = \log_a c$

$\log_a b = \frac{1}{\log_b a}$

Characteristic Polynomial Of Linear Recurrence

Complex Numbers

$e^{ia} = \cos(a) + i\sin(a)$

$a^2+b^2 = (a+ib)(a-ib)$

$(P(x)+iQ(x))(P(x)-iQ(x)) =$
$\prod_{j=0}^{n-1}\left(x - e^{2\pi i\frac{2j+1}{4n}}\right)\prod_{j=0}^{n-1}\left(x + e^{2\pi i\frac{2j+1}{4n}}\right)$
Choose 1 out of 2 from each j for complex conjugacy and degree.

Gauss-Lucas: the roots of the derivative of a complex polynomial lie in the convex hull of the roots of the original polynomial.

Enestrom-Kakeya: if
$f(x) = a_0 + a_1x + \cdots + a_nx^n$ with real
$0 \leq |a_0| \leq |a_1| \leq |a_2| \leq \cdots \leq |a_n|$ then every root satisfies $|z| \leq 1$

Discrete And Continuous/Integral Inequalities

By continuity it suffices to prove this for the Riemann sum and pass to the limit.

Trivial Inequality: $x^2 \geq 0$

AM-GM: $\frac{\sum a_i}{n} \geq \left(\prod a_i\right)^{\frac{1}{n}}$
$\sum a_i \geq n\left(\prod a_i\right)^{\frac{1}{n}}$

Cauchy-Schwarz:
$\left(\sum a_i^2\right)\left(\sum b_i^2\right) \geq \left(\sum a_ib_i\right)^2$

Jensen: convex f, $a_i \geq 0$, $\sum a_i = 1$,

$\sum a_i f(x_i) \geq f\left(\sum a_i x_i\right)$

Minkowski: $p > 1$,
$(\sum |a_i + b_i|^p)^{\frac{1}{p}} \leq (\sum |a_i|^p)^{\frac{1}{p}} + (\sum |b_i|^p)^{\frac{1}{p}}$
and the reverse for $p < 1$ and $a_i, b_i \geq 0$

Holder: $\frac{1}{p} + \frac{1}{q} = 1$,
$(\sum a_i^p)^{\frac{1}{p}} (\sum b_i^q)^{\frac{1}{q}} \geq \sum a_i b_i$
And In General e.g.
$\frac{1}{p} + \frac{1}{q} + \cdots + \frac{1}{r} = 1$,
$(\sum a_i^p)^{\frac{1}{p}} (\sum b_i^q)^{\frac{1}{q}} \ldots (\sum c_i^r)^{\frac{1}{r}} \geq$
$\sum a_i b_i \ldots c_i$

Chebyshev: $a_1 \geq a_2 \geq \cdots \geq a_n$,
$b_1 \geq b_2 \geq \cdots \geq b_n$,
$n \sum a_i b_i \geq (\sum a_i)(\sum b_i)$ and vice versa for anti ordered.

Schur: non negative $x^t(x-y)(x-z) + y^t(y-z)(y-x) + z^t(z-x)(z-y) \geq 0$

Muirhead: a_i positive reals and x_n majorises y_n,
$\sum_{\text{sym}} a_1^{x_1} a_2^{x_2} \ldots a_n^{x_n} \geq \sum_{\text{sym}} a_1^{y_1} a_2^{y_2} \ldots a_n^{y_n}$

Majorises:
$x_1 \geq y_1, x_1 + x_2 \geq y_1 + y_2, \ldots,$
$x_1 + x_2 + \cdots + x_n = y_1 + y_2 + \cdots + y_n$

Tangent Line Trick i.e. Taylor's Theorem Convex:
$f(x) \geq f(a) + f'(a)(x-a)$

Functional Equations: plug in 0, 1, x, $f(x)$ i.e. ad hoc de novo injective, surjective, bijective, monotone, continuity, equality, canceling, substitutions, guessing, involution (tripling and un doubling e.g.), isolated parts, swapping, transformations, confirm solutions.

Cauchy: $f(x+y) = f(x) + f(y)$ over $\mathbb{Q}$ implies $f(x) = kx$ or over $\mathbb{R}$ if continuous in any interval, bounded in any nontrivial interval, or omits some nontrivial disk.

Jensen: $f(x) + f(y) = 2f\left(\frac{x+y}{2}\right)$ over $\mathbb{Q}$ implies $f(x) = kx$

Dirichlet: remainders modulo 1 of integer multiples of an irrational a are dense in $[0, 1]$ i.e. $a, 2a, 3a, \ldots \pmod 1$

Arithmetic Series: $n \cdot \frac{a_1 + a_n}{2}$

Geometric Series: $\frac{a_1}{1-r}$ or
$\frac{a_1 - a_{n+1}}{1-r} = \frac{a_1(1-r^n)}{1-r}$

Arithmetico-Geometric Series: break in to a sum of geometric series
$\frac{ab-(a+nd)br^n}{1-r} + \frac{dbr(1-r^n)}{(1-r)^2}$ or $\frac{ab}{1-r} + \frac{dbr}{(1-r)^2}$

Swapping Sum Order (In General For Many Try Different)

Telescoping

Induce Symmetry

$x \to \frac{x-1}{x} \to \frac{-1}{x-1} \to x$

Create Cyclic Sets/Partitions

Creating Sets To Exploit i.e. Cyclic Shifts

Creating Symmetric Sets

Bezout: 2 curves in $\mathbb{P}^2(\mathbb{C})$ of degrees m, n and not sharing any common component meet in exactly mn points when counted with multiplicity.

Binomial: for $\binom{r}{k} = \frac{r(r-1)...(r-k+1)}{k!}$
$(x+y)^r = \sum_{k=0}^{\infty} \binom{r}{k} x^{r-k} y^k =$
$x^r + rx^{r-1}y + \frac{r(r-1)}{2!}x^{r-2}y^2 + \dots$

Chebyshev: $T_n(x) = \cos(n \cdot \arccos(x))$
$T_0(x) = 1, T_1(x) = x, T_{n+1}(x) =$
$2xT_n(x) - T_{n-1}(x)$
$1, x, 2x^2 - 1, 4x^3 - 3x, 8x^4 - 8x^2 + 1, \dots$
The polynomial $2^{-n+1}T_n(x)$ is the unique monic nth degree polynomial satisfying
$\frac{1}{2^{n-1}} = \max_{-1 \le x \le 1} |2^{-n+1}T(x)| \le$
$\max_{-1 \le x \le 1} |P(x)|$ for any other monic nth degree polynomial $P(x)$

Distributions And Statistics

Bernoulli Distribution: $[0, 1]$ with $[1-p, p]$
E[Bernoulli] $= p$
Var[Bernoulli] $= p(1-p)$
$P_X(s) = ps + q$
$m_Y(t) = (1-p) + pe^t$

Binomial Distribution (n, p):
$[0, 1, \dots, n]$ with $[\binom{n}{0}p^0(1-p)^n, \dots]$
E[Binomial(n,p)] $= np$
Var[Binomial(n,p)] $= np(1-p)$
$P_X(s) = (ps+q)^n$
$m_Y(t) = (pe^t + (1-p))^n$

Geometric Distribution: $[0, 1, 2, \dots]$ with $[p, p(1-p), p(1-p)^2, \dots]$
E[Geometric] $= \frac{1-p}{p}$
Var[Geometric] $= \frac{1-p}{p^2}$
$P_X(s) = \frac{p}{1-qs}$
$m_Y(t) = \frac{p}{1-(1-p)e^t}$

Poisson Distribution: $[0, 1, 2, \dots]$ with $[e^{-\lambda}\frac{\lambda^k}{k!}]$
E[Poisson] $= \lambda$
Var[Poisson] $= \lambda$
$P_X(s) = e^{\lambda(s-1)}$
$m_Y(t) = e^{\lambda(e^t-1)}$

Uniform Distribution $[a, b]$:
$f_Y(y) = \frac{1}{b-a}1_{[a,b]}(y)$
E$[Y] = \frac{a+b}{2}$
Var$[Y] = \frac{(b-a)^2}{12}$
$F_Y(y) = \frac{y-a}{b-a}$ for $y \in [a, b]$
$m_Y(t) = \frac{e^{bt}-e^{at}}{t(b-a)}$
$\mu_k = \frac{b^{k+1}-a^{k+1}}{(k+1)(b-a)}$

Normal Distribution $Y \sim N(\mu, \sigma)$:
$y\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(y-\mu)^2}{2\sigma^2}}$
E$[Y] = \mu$
Var$[Y] = \sigma^2$
$\mu_k^c = \sigma^k(k-1)(k-3)\dots(1)$ and $\mu_k^c = 0$ for odd k
$m_Y(t) = e^{\mu t + \frac{1}{2}\sigma^2 t^2}$

Exponential Distribution $\tau > 0$:
$f_Y(y) = \frac{1}{\tau}e^{-\frac{y}{\tau}}1_{[0,\infty)}(y)$
E$[Y] = \tau$
Var$[Y] = \tau^2$
$\mu_k = k!t^k$
$S(y) = e^{-\frac{y}{\tau}}$
$h(y) = \frac{1}{\tau}$
$F_Y(y) = 1 - e^{-\frac{y}{\tau}}$ for $y > 0$
$m_Y(t) = \frac{1}{1-\tau t}$

$\chi^2(n)$ Distribution:
$f_Y(y) = \frac{1}{2^{\frac{n}{2}}\Gamma(\frac{n}{2})}y^{\frac{n}{2}-1}e^{-\frac{y}{2}}$
E$[Y] = n$
Var$[Y] = 2n$
$F_Y(y) = \frac{1}{\Gamma(\frac{n}{2})}\gamma(\frac{n}{2}, \frac{y}{2})$
$m_Y(t) = (1-2t)^{-\frac{n}{2}}$

$\Gamma(k,\tau)$ Gamma Distribution:
$f_Y(y) = \frac{1}{\Gamma(k)\tau^k} y^{k-1} e^{-\frac{y}{\tau}}$
$\mathrm{E}[Y] = k\tau$
$\mathrm{Var}[Y] = k\tau^2$
Exponential $E(\tau) = \Gamma(1,\tau)$ and
$\chi^2(n) = \Gamma(\frac{n}{2}, 2)$
$m_Y(t) = (1-\tau t)^{-k}$

$\mathrm{E}[Y] = \int_{-\infty}^{\infty} y f_Y(y) dy$ when well defined

$\mathrm{Var}[Y] = \int_{-\infty}^{\infty} (y-\mu_y)^2 f_Y(y) dy$ with
$\mu_Y = \mathrm{E}[Y]$ mean/expectation of Y

$\mathrm{Cov}(X,Y) = \mathrm{E}[(X - \mathrm{E}[X])(Y - \mathrm{E}[Y])] =$
$\mathrm{E}[XY] - \mathrm{E}[X]\mathrm{E}[Y]$

k-th Moment (Raw):
$\mu_k = \mathrm{E}[Y^k] = \int_{-\infty}^{\infty} y^k f_Y(y) dy$

k-th Central Moment: $\mu_k^c =$
$\mathrm{E}[(Y - \mathrm{E}[Y])^k] = \int_{-\infty}^{\infty} (y-\mu)^k f_Y(y) dy$

Note Standardised Moment is Central Moment normalised typically with division by an expression of the Variance which renders the moment scale invariant.

Expectation/Mean $\mu = \mu_1 = \mathrm{E}[Y]$

Variance $\mu_2^c = \mathrm{Var}[Y]$

Skewness $\mathrm{E}\left[\frac{Y - \mathrm{E}[Y]}{\mathrm{sd}[Y]}^3\right] = \frac{\mu_3^c}{(\mu_2^c)^{\frac{3}{2}}}$

Kurtosis $\mathrm{E}\left[\frac{Y - \mathrm{E}[Y]}{\mathrm{sd}[Y]}^4\right] = \frac{\mu_4^c}{(\mu_2^c)^2}$

Cumulative Distribution Function [cdf]:
$F(y) = P[Y \leq y]$

$F(y) = \int_{-\infty}^{y} f(z) dz$

$f(y) = F'(y)$

Survival Function: $S(y) = 1 - F(y)$

Hazard Function: $h(y) = \frac{f(y)}{S(y)}$ roughly the conditional probability that the individual will die at time y given that it has survived until y

cdf-Method: $W = g(Y)$ want
$F_W(w) = P[g(Y) \leq w] = P[Y \leq g^{-1}(w)] = F(g^{-1}(w))$

Inverse Exponential Distribution:
$f(y) = \frac{1}{ty^2} e^{-\frac{1}{ty}} 1_{(0,\infty)}(y)$
$F(y) = e^{-\frac{1}{ty}}$

χ^2 Distribution:
$f(y) = \frac{1}{\sqrt{2\pi y}} e^{-\frac{y}{2}} 1_{(0,\infty)}(y)$

$f_W(w) = f_Y(g^{-1}(w)) |(g^{-1})'(w)|$

Law Of Large Numbers: if $X_1, X_2, \ldots$ is an infinite sequence of independent and identically distributed Lebesgue integrable random variables with expected value
$E(X_1) = E(X_2) = \cdots = \mu$ then the sample average
$\hat{X}_n = \frac{1}{n}(X_1 + X_2 + \cdots + X_n)$ converges to the expected value e.g. for any $\epsilon_1, \epsilon_2 > 0$ there exists an N such that for $n > N$ the probability that $\hat{X}_n \in [\mu - \epsilon_1, \mu + \epsilon_1]$ is at least $1 - \epsilon_2$

Differential Equations

$y' + p(t)y = g(t)$
$u(t)y' + u(t)p(t)y = u(t)g(t)$
Integrating Factor $u(t)$ Satisfies
$u(t)p(t) = u'(t)$
$\frac{u'(t)}{u(t)} = p(t)$
$(\ln(u(t)))' = p(t)$
$\ln(u(t)) = \int p(t)dt + c$
$u(t) = e^{\int p(t)dt+c} = e^c e^{\int p(t)dt} = ce^{\int p(t)dt}$
$u(t)y' + u'(t)y = (u(t)y(t))' = u(t)g(t)$
$u(t)y(t) + c = \int u(t)g(t)dt$
$y(t) = \frac{\int u(t)g(t)dt+c}{u(t)}$

$N(y)\frac{dy}{dx} = M(x)$
$\int N(y)dy = \int M(x)dx$

$M(x,y) + N(x,y)\frac{dy}{dx} = 0$
If $F_x + F_y\frac{dy}{dx} = 0$
$\frac{d}{dx}(F(x,y(x))) = 0$
$F(x,y) = c$
Check $F_{xy} = F_{yx}, M_y = N_x$
Perhaps Solve

Bernoulli Equations
$y' + p(x)y = q(x)y^n$
$y^{-n}y' + p(x)y^{1-n} = q(x)$
$v = y^{1-n}$
$v' = (1-n)y^{-n}y'$
$\frac{1}{1-n}v' + p(x)v = q(x)$
$v' + (1-n)p(x)v = (1-n)q(x)$
Solve Linear Equation And Solve For y

Substitutions

$y' = f\left(\frac{y}{x}\right)$
Homogeneous Equations
$v(x) = \frac{y}{x}$
$y = xv$
$y' = v + xv'$
$v + xv' = f(v)$
$xv' = f(v) - v$
$\frac{1}{f(v)-v}dv = \frac{1}{x}dx$
$x = ce^{\int \frac{1}{f(v)-v}dv}$

$y' = g(ax + by)$
$v = ax + by$
$v' = a + by'$
$\frac{1}{b}(v' - a) = g(v)$
$v' = a + bg(v)$
$\frac{1}{a+bg(v)}dv = dx$
$x = \int \frac{1}{a+bg(v)}dv + c$

Logistic Growth
$P' =$
(Growth Rate) $\left(1 - \frac{P}{\text{Saturation Level}}\right) P$
$P(t) = 0, P(t) =$ Saturation Level
Unstable/Stable Equilibria

Euler, Runge-Kutta Methods, Assert Maximum Error Bound Obtained, Error $\Theta(h)$ Of Step Size

$ay'' + by' + cy = 0$
$ar^2 + br + c = 0$
Distinct Real
$y(t) = c_1e^{r_1t} + c_2e^{r_2t}$
Complex (Roots $a \pm ib$) (Same As Real)
$y(t) = c_1e^{at}\cos(bt) + c_2e^{at}\sin(bt)$
Repeated Roots
$y(t) = c_1e^{rt} + c_2te^{rt}$

Reduction Of Order
Given $y_1(t)$ Solution Solve
$y_2(t) = v(t)y_1(t)$

For particular solutions ad hoc inspect functions related to the right hand side functions. For computing mutual antiderivative inspect terms which

would produce such a term, and note degrees of terms which can match e.g.

Undetermined Coefficients
Variation Of Parameters
Solve $y(t) = u_1(t)y_1(t) + u_2(t)y_2(t)$
From Homogeneous Solutions

$a_n\frac{d^n y}{dx^n} + \cdots + a_2\frac{d^2y}{dx^2} + a_1\frac{dy}{dx} + a_0 = f(x)$
Characteristic Equation:
$a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 = 0$
General Solution To Homogeneous Differential Equation:
$y(x) =$
$P_1(x)e^{\lambda_1 x} + P_2(x)e^{\lambda_2 x} + \cdots + P_r(x)e^{\lambda_r x}$
$P_i(x)$ is a polynomial of degree 1 less than the multiplicity of λ_i

Combinatorics

Bijections

Binary, Ternary, etc. Strings

Block Walking Argumentation

$\sum \binom{n}{a}^2 = \binom{2n}{n}$

$\sum \binom{a}{1}\binom{n-1-a}{2} = \binom{n}{4}$ by case work on the index of the 2nd element in the subset e.g.

$\sum_{k\geq 0} \binom{n-k}{k} = F_{n+1}$

Twelvefold Way

Pascal's Triangle:
1
1, 1
1, 2, 1
1, 3, 3, 1
1, 4, 6, 4, 1
1, 5, 10, 10, 5, 1
1, 6, 15, 20, 15, 6, 1
1, 7, 21, 35, 35, 21, 7, 1
1, 8, 28, 56, 70, 56, 28, 8, 1
1, 9, 36, 84, 126, 126, 84, 36, 9, 1
1, 10, 45, 120, 210, 252, 210, 120, 45, 10, 1
1, 11, 55, 165, 330, 462, 462, 330, 165, 55, 11, 1
...

Binomial: a choose b i.e. splitting a set of a elements in to 2 sets of size b and $a - b$ is $\binom{a}{b} = \frac{a!}{b!(a-b)!}$

Multinomial: a choose $b_1, b_2, \ldots, b_n$ i.e. splitting a set of a elements in to n sets of sizes b_i is $\binom{a}{b_1,\ldots,b_n} = \frac{a!}{b_1!b_2!\ldots b_n!}$

Catalan:

$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, \ldots$
$C_n = \frac{1}{n+1}\binom{2n}{n}$ e.g. parentheses, non intersecting chords, etc.

Counting In 2 Ways

Choose Extremal

Incidences

Pigeonhole Principle: there exists a box with at least $\left\lceil \frac{b}{a} \right\rceil$ balls.

Principle Of Inclusion-Exclusion:
$|\cup A_i| = \sum |A_i| - \sum |A_i \cap A_j| +$
$\sum |A_i \cap A_j \cap A_k| - \ldots$

Count Symmetric Multiplicities And Sums

Bonferroni: partial sums in Principle Of Inclusion-Exclusion alternate between $\geq$ and $\leq$ true value.

Number Of Permutations With r Fixed Points: $\frac{n!}{r!}(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^{n-r}}{(n-r)!})$

Inversion: if $b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$ then
$a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k$

Uniform Random n Points Cutting Unit Interval Symmetry Isomorphism With Uniform Random $n+1$ Points Cutting Unit Circle:
Intervals Have Same Distribution
$f(x) = n(1-x)^{n-1}$
Expected Values Of Sorted:
Smallest $\frac{1}{n}\left(\frac{1}{n}\right)$
2nd Smallest $\frac{1}{n}\left(\frac{1}{n} + \frac{1}{n-1}\right)$
3rd Smallest $\frac{1}{n}\left(\frac{1}{n} + \frac{1}{n-1} + \frac{1}{n-2}\right) \ldots$
Largest $\frac{1}{n}\left(\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{2} + 1\right)$

Algorithms

Point Sets Splitting Lines, Windmills, Directional $a, (b-a)$ Line Splitting, Continuous Rotational Intermediate Value Argumentation

Monovariants And Invariants

Symmetry, Pairing, Copying

Tiling In General Modulo, Complex, Continuous

Parity

Burnside: $X/G = \frac{1}{|G|} \sum_{g \in G} |X^g|$

Generating Functions

Generating Functionology

$a_{n+1} + ua_n + va_{n-1} = 0$
$G(x) - a_0 - a_1 x + ux(G(x) - a_0) +$
$vx^2 G(x) = 0$
$G(x) = \frac{a_0 + (ua_0 + a_1)x}{1 + ux + vx^2}$
$G(x) = \frac{\alpha}{1 - r_1 x} + \frac{\beta}{1 - r_2 x} =$
$\sum_{n=0}^{\infty} (\alpha r_1^n + \beta r_2^n) x^n$

$(1+x)^n = \sum_{k \geq 0} \binom{n}{k} x^k$

$\frac{1}{(1-x)^{m+1}} = \sum_{k \geq 0} \binom{k+m}{m} x^k$

$\frac{x^m}{(1-x)^{m+1}} = \sum_{k \geq 0} \binom{k}{m} x^k$

$\frac{1}{\sqrt{1-4x}} = \sum_{k \geq 0} \binom{2k}{k} x^k$

$\frac{1-\sqrt{1-4x}}{2x} = \sum_{k \geq 0} C_k x^k$

$e^x = \sum_{k \geq 0} \frac{1}{k!} x^k$

Same Number Of Partitions In To Odd Parts And Distinct Parts

Bijection Method

Generating Function Method

$\prod_{k=1}^{\infty}(1+x^k) =$
$\prod_{k=1}^{\infty}((1+x^{2k-1})(1+x^{2(2k-1)})(1+$
$x^{4(2k-1)})\dots) =$
$\prod_{k=1}^{\infty}(1+x^{2k-1}+x^{2(2k-1)}+x^{3(2k-1)}+\dots)$
Where the left hand side is the generating function for the number of partitions in to distinct parts and the right hand side is the generating function for the number of partitions in to odd parts.

Prove $\sum_{j=0}^{n}\binom{n}{j}2^{n-j}\binom{j}{\lfloor\frac{j}{2}\rfloor} = \binom{2n+1}{n}$
$\binom{j}{\lfloor\frac{j}{2}\rfloor}$ is the constant term in
$(1+x)(x^{-1}+x)^j$
Constant term in
$\sum_{j=0}^{n}\binom{n}{j}2^{n-j}(1+x)(x^{-1}+x)^j$
$= (1+x)\sum_{j=0}^{n}\binom{n}{j}(x^{-1}+x)^j 2^{n-j} =$
$(1+x)(2+x^{-1}+x)^n$
$= \frac{1}{x^n}(1+x)(2x+1+x^2)^n =$
$\frac{1}{x^n}(1+x)^{2n+1} \to \binom{2n+1}{n}$

Snake Oil Method

Impose Structure And Order Create Useful Sets

The Probabilistic Method

$\mathrm{E}[X] < 1$ implies there exists a setting with $X = 0$ e.g. and very concretely if the support of X is on $0, 1, 2, \dots$ then $\mathrm{E}[x] = p < 1$ means at least weight $1-p$ lies on 0 by smoothing. Also, if ≥ 1 prisoner must guess correctly to avoid mass execution then the union of the events of correct guesses is relevant and the lower the intersections, the better.

For any set of 10 points in $\mathbb{R}^2$, there exists a set of non intersecting unit disks which covers it.

Union Bound: $P(\cup A_i) \leq \sum P(A_i)$

Partially Ordered Set

Width

Dilworth: the size of the largest antichain in a partial order equals the smallest number of chains in to which the order may be partitioned.

Mirsky: the size of the largest chain in a partial order equals the smallest number of antichains in to which the order may be partitioned.

Konig: in any bipartite graph, the number of edges in a maximum matching equals the number of vertices in a minimum vertex cover.

Vertex Cover: set of vertices which hits every edge.

Intervals: $mn+1$ closed intervals in $\mathbb{R}$, either there are $m+1$ intervals that are pair wise disjoint or there are $n+1$ intervals with a non empty intersection.

Erdos-Szekeres: sequence of $mn+1$ distinct real numbers contains a monotonically increasing subsequence of length $m+1$ or a monotonically decreasing subsequence of length $n+1$

Sperner: if F is a family of subsets of

$1, 2, \ldots, n$ such that no subset contains another i.e. an antichain then $|F| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ with equality by taking all sets of size $\lfloor \frac{n}{2} \rfloor$

Brouwer: let B^n denote an n-dimensional ball. For any continuous map $f : B^n \to B^n$, there is a point $x \in B^n$ such that $f(x) = x$

Erdos: for any set X of distinct integers, X has a sum-free subset Y with $|Y| > \frac{|X|}{3}$

Linearity Of Expectation: $E[X_1 + X_2 + \cdots + X_n] = E[X_1] + E[X_2] + \cdots + E[X_n]$

If X, Y are independent random variables then $E[XY] = E[X]E[Y]$

Markov: if X is a random variable taking nonnegative values and if $a > 0$, then $P(X \geq a) \leq \frac{1}{a}E[X]$

Chebyshev: let X be a random variable and let $a > 0$, then $P(|X - E[X]| \geq a) \leq \frac{1}{a^2}(E[X^2] - E[X]^2)$

Szele: there exists a tournament with n players which has at least $\frac{n!}{2^{n-1}}$ Hamiltonian paths.

$\binom{n}{k} < \frac{1}{e}\left(\frac{en}{k}\right)^k$

Lovasz: events each occurring with probability $\leq p$ such that each event is independent of all the others except at most d then $epd < 1$ implies the probability 0 events occur is positive e.g. Russian tourist camp t-shirt colour example.

Graph Theory

Graph transformations and interpretations such as rows and columns as vertex sets forming a bipartite graph with an edge if and only if a something corresponding, a corresponding graph where the edges are the vertices and there is an edge if and only if they share a vertex in the original graph, a dual graph where the faces are the vertices and the edges are if they shared an edge etc. e.g. maybe some task where a function takes a graph A to B, B to C, and C to A then note something.

Hall: A and B bipartite with any subset $C \in A$ having $|C| \leq |N_G(C)|$ i.e. every subset of A has sufficiently many adjacent vertices in B then there exists an A-perfect matching i.e. a matching with every vertex in A uniquely matched.

Mantel: a triangle free graph G on n vertices contains $|E| \leq \frac{n^2}{4}$

A graph with n vertices and k edges has at least $\frac{k}{3n}(4k - n^2)$ triangles.

Zarankiewicz: in any graph with no K_r subgraph there exists a vertex with degree at most $\lfloor \frac{r-2}{r-1}n \rfloor$

Turan: in any graph with no K_{k+1} subgraph $|E| \leq \frac{(k-1)n^2}{2k}$

Caro-Wei: the maximum size

independent set has size
$\alpha(G) \geq \sum_{v \in V} \frac{1}{d_v+1}$

Ramsey: $R(s,t) \leq \binom{s+t-2}{s-1}$ such that for every $N \geq R(s,t)$, every 2 colouring of the complete graph K_N must contain either a red copy of K_s or a blue copy of K_t

Schur: for all r there is a number $S(r)$ such that any r-colouring of $\{1, 2, \ldots, S(r)\}$ has a monochromatic solution to $x + y = z$

If the set $\{1, 2, \ldots, 1978\}$ is partitioned in to 6 sets, then in one of these sets there are a, b, c such that $a + b = c$.
Proof: otherwise by pigeonhole say A has 330 elements $a_1 < a_2 < \cdots < a_{330}$, then it does not contain the differences $a_{330} - a_{329}, a_{330} - a_{328}, \ldots, a_{330} - a_1$ and again by pigeonhole say B contains 66 of those, iterated etc.

For any k, r, l there is a least integer $\mathrm{HR}(k, l, r)$ such that if $n \geq \mathrm{HR}(k, l, r)$ and all the k-subsets of an n-set S are r-coloured, then all the k-subsets of some l-subset of S have the same colour.

Let P be a set of 5 points in $\mathbb{R}^2$ with no 3 on a line. Then some subset of 4 points of P forms a convex 4-gon.

Let P be a set of n points in $\mathbb{R}^2$, such that each 4-tuple forms a convex 4-gon. Then P forms a convex n-gon.

For all n there exists an integer N such that, if P is a set of at least N points in $\mathbb{R}^2$, with no three points on a line, then P contains a convex n-gon.
Proof: Suppose $n \geq 5$ and take $N = \mathrm{HR}(4, n, 2)$. colour the 4-subsets of P red if they form a convex set and blue otherwise. There is no 5-subset for which all 4-subsets are blue. Hence there must exist an n-subset all of whose 4-subsets are red.

Euler: there exists a cycle/path using each edge exactly once if and only if G is connected and every/all-but-2 vertex/vertices of G has even degree. Or in the case of a directed graph when all the edges belong to the same strongly connected component and the indegree equals the outdegree for each vertex or for 1 it is 1 larger and for 1 it is 1 smaller e.g.

Dirac-Ore: if G is simple, with $n \geq 3$ vertices, and $\deg u + \deg v \geq n$ for every 2 non adjacent vertices u, v then G has a Hamiltonian cycle.

Hamiltonian Cycle/Path: a cycle/path through every vertex.

If $X \subset V(G)$ and $G - X$ has $> |X|$ connected components, then G has no Hamiltonian cycle.

Spanning Tree: T of G if T is a tree and $V(T) = V(G)$, every connected graph G has a spanning tree.

Fundamental Cycle Of f With Respect To T: for an edge $f \in E(G) - E(T)$ note that $T \cup \{f\}$ contains precisely 1 cycle, and if C is this fundamental cycle

then for every $e \in E(C) - \{f\}$, we have that $T + f - e$ is a spanning tree of G

Number of rooted forests on n vertices with k fixed roots is kn^{n-k-1}

Cayley: n^{n-2}

Laplacian Matrix: $L = D - A$ where D is diagonal degree matrix and A is the adjacency matrix with all diagonal entries 0

Kirchhoff: the number of spanning trees for a given connected graph G with n labeled vertices and non zero eigenvalues of its Laplacian matrix $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ is $\frac{1}{n}\lambda_1\lambda_2 \ldots \lambda_{n-1}$

Planar: when a graph can be drawn in such a way that no 2 edges intersect each other.

Kuratowski: a graph G is planar if and only if G does not contain a subgraph which is a subdivision of K_5 or $K_{3,3}$

Every simple, connected, planar graph is 4-colourable.

Elekes: for any finite set of real numbers A we have $|A + A| \cdot |A \cdot A| \geq \frac{1}{32}|A|^{\frac{5}{2}}$

Enumerative

Permutations

Sign Of π: $(-1)^{\text{number of inversions}}$, $\prod \frac{\pi(x)-\pi(y)}{x-y}$, parity of number of cycles of even length.

Prefix/Partial Sums And Subsequence Sums

Stochastic Processes

Write transition matrix P in the canonical form:
$\begin{bmatrix} PC & 0 \\ R & Q \end{bmatrix}$

So Q is T to T edges and PC is C to C edges and R is T to C edges where T is transient states i.e. union of all transient classes and PC is recurrent/closed states i.e. union of all sink connected components whence:

$U = (1 - Q)^{-1}R =$
$(1 + Q + Q^2 + \ldots)R = FR$ is transition probabilities

F captures expected number of times hitting each state in T prior to transitioning into C

Markov Chains

State Based Recurrences e.g. Expected Number Of Steps

Game Theory

Positional Analysis

Nash Equilibria: no agent incentivised to deviate

Sprague-Grundy: $\text{mex}(g_1, g_2, \ldots, g_n)$

Incidence Matrices

Counting Pairs And Triples

Tournament e.g. $\sum w_i^2 = \sum l_i^2$

Erdos-Ko-Rado: if F is a family of k-element subsets of $1, 2, \ldots, n$ such

that every 2 sets in F have nontrivial intersection then $|F| \leq \binom{n-1}{k-1}$

Combinatorial Geometry

Euler Characteristic:
$V - E + F = 2 - 2g$

Platonic Solids: Faces are congruent regular polygons and each vertex belongs to the same number of edges.
Tetrahedron: $V = 4, E = 6, F = 4$
Cube: $V = 8, E = 12, F = 6$
Dodecahedron: $V = 20, E = 30, F = 12$
Octahedron: $V = 6, E = 12, F = 8$
Icosahedron: $V = 12, E = 30, F = 20$

Convex Hull: of points x_i is the set of points $\sum w_i x_i$ with $w_i \geq 0$ and $\sum w_i = 1$

Minkowski: every origin symmetric convex set in $\mathbb{R}^n$ with volume greater than 2^n contains a nontrivial integer point.

Radon: a set of $n + 2$ points in $\mathbb{R}^n$ can be partitioned in to 2 sets with intersecting convex hulls.

Caratheodory: a point in a convex hull in $\mathbb{R}^n$ is the convex combination of some set of $n + 1$ points in the convex hull.

Helly: a finite set of $\geq n + 1$ convex sets in $\mathbb{R}^n$ such that every $n + 1$ has nonempty intersection has nonempty intersection, and for infinitely many if compact.

Hahn-Banach: for 2 non-intersecting convex bodies there exists a hyperplane which separates them.

Sperner: if each vertex of an n-dimensional simplex is coloured with a distinct colour and it is dissected into n-dimensional simplices such that each vertex on a face is 1 of the colours of the vertices on that face then there exist an odd number of simplices in the dissection whose vertices all have distinct colours in particular there exists at least 1 such simplex.

Sylvester-Gallai: for any finite non-collinear set of points in $\mathbb{R}^2$ there exists a line passing through precisely 2

Erdos: every n points in $\mathbb{R}^2$ which are not all collinear must determine at least n distinct lines.

Stone-Tukey: any n sets in $\mathbb{R}^n$ can be simultaneously bisected by an $(n - 1)$ dimensional hyerplane.

Example: each of 100 baskets contains some number (could be zero) of apples, some number of bananas, and some number of cherries. Show that you can collect 51 of those baskets that together contain at least half the apples, at least half the bananas, and at least half the cherries!

Geometry

Area: $S = \frac{bh}{2} = rs = \frac{ab\sin(\theta)}{2} = \frac{abc}{4R} = \sqrt{s(s-a)(s-b)(s-c)}$

Power Of A Point: $AB \cdot AC$

Angle Bisector Theorem: $\frac{AB}{AC} = \frac{DB}{DC}$

Ratio Lemma: $\frac{DB}{DC} = \frac{AB}{AC} \cdot \frac{\sin(DAB)}{\sin(DAC)}$

Law Of Sines:
$\frac{a}{\sin(A)} = \frac{b}{\sin(B)} = \frac{c}{\sin(C)} = 2R$

Law Of Cosines:
$c^2 = a^2 + b^2 - 2ab\cos(C)$
$\cos(C) = \frac{a^2+b^2-c^2}{2ab}$

Arcs And Angles In Circle: 1 or $\frac{1}{2}$ measure subtended arc.

Stewart: $dad + man = bmb + cnc$

Bretschneider: $S = ((s-a)(s-b)(s-c)(s-d) - abcd\cos^2(\theta))^{\frac{1}{2}}$ where $\theta = \frac{A+C}{2}$

Cyclic Quadrilateral If And Only If $A + C = \pi = B + D$

Ptolemy: $ef = ac + bd$ for cyclic quadrilateral.

Ceva: $\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1$ for D, E, F on AB, BC, CA with AD, BE, CF concurrent.

Menelaus: $\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = -1$ for D, E, F on AB, BC, CA with D, E, F collinear.

Pick: Lattice Points
$S = \text{Interior} + \frac{\text{Boundary}}{2} - 1$

Shoelace: $\frac{1}{2} \cdot \sum(a_i b_{i+1} - a_{i+1} b_i)$

Isoperimetric Inequality: ball maximises $\frac{\text{Volume}}{\text{Surface Area}}$

Isodiametric Inequality: ball maximises Volume.

9-Point Circle: homothety of circumcircle with center orthocenter and ratio $\frac{1}{2}$, midpoints of sides AB, BC, CA, bases of altitudes, midpoints of AH, BH, CH

$s - a, s - b, s - c \to$
$a = y + z, b = z + x, c = x + y$

Incircle And Incenter At Concurrency Of Angle Bisectors, Excircles

Circumcenter At Concurrency Of Perpendicular Bisectors

Orthocenter At Concurrency Of Altitudes

Pyramid: $V = \frac{bh}{3}$

$r = 4R\sin\left(\frac{A}{2}\right)\sin\left(\frac{B}{2}\right)\sin\left(\frac{C}{2}\right)$

$1 + \frac{r}{R} = \cos(A) + \cos(B) + \cos(C)$

$1 + 4\sin\left(\frac{A}{2}\right)\sin\left(\frac{B}{2}\right)\sin\left(\frac{C}{2}\right) = \cos(A) + \cos(B) + \cos(C)$

Circle: $0 = \begin{vmatrix} x^2+y^2 & x & y & 1 \\ x_1^2+y_1^2 & x_1 & y_1 & 1 \\ x_2^2+y_2^2 & x_2 & y_2 & 1 \\ x_3^2+y_3^2 & x_3 & y_3 & 1 \end{vmatrix}$

3-Sphere: $V = \frac{4\pi r^3}{3}$, $S = 4\pi r^2$

Multivariable

n-Sphere: $V_0 = 1$, $S_0 = 2$, $V_{n+1} = \frac{S_n}{n+1}$, $S_{n+1} = 2\pi V_n$, $V_n = \frac{\pi^{\frac{n}{2}}}{(\frac{n}{2})!}$ where i.e. $(\frac{5}{2})! = \pi^{\frac{1}{2}} \cdot \frac{5}{2} \cdot \frac{3}{2} \cdot \frac{1}{2}$

Positive Region Bound By $x + y + \cdots = 1$: $V = \frac{1}{n!}$

Simplex volume from paralleliped volume as $\frac{\det(A)}{n!}$ where A is an $n \times n$ matrix of offset vectors from a vertex.

Largest k-dimensional ball inside an n-dimensional unit hypercube has radius $\frac{1}{2}\sqrt{\frac{n}{k}}$

Coordinate Bashing

Analytic Techniques

Mass Points

Collinearity $\iff$ Equal Slopes $\iff$ $S = 0$

Conic: $ax^2 + by^2 + cxy + dx + ey + f = 0$
Except in the degenerate case of 2 parallel lines it can be obtained by sectioning a circular cone by a plane. Degenerate are pairs of lines, single points, the entire plane, and the empty set.
Parabola: $y^2 = 4px$
Ellipse: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$
Hyperbola: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$

The sum of the squares of the lengths of n mutually perpendicular chords through a fixed point P inside an n-dimensional sphere is, irrespective of directions,
$\sum ||X_iY_i||^2 = 4nR^2 - 4(n-1)||PO||^2$

A disk of radius R is covered by m rectangular strips of width 2, $m \geq R$

Archimedes: The area of the surface cut from a sphere of radius R by 2 parallel planes at distance d from each other is equal to $2\pi Rd$

Torus: $V = (\pi r^2)(2R\pi) = 2\pi^2 Rr^2$
$S = (2r\pi)(2R\pi) = 4\pi^2 Rr$

Pascal: for 6 points on a conic $AB \cap DE, BC \cap EF, CD \cap FA$ are collinear.

Desuarge: two triangles are in perspective axially if and only if they are in perspective centrally. Aa, Bb, Cc are concurrent at the center of perspectivity if and only if $AB \cap ab, BC \cap bc, CA \cap ca$ are collinear on the axis of perspectivity.

Poncelet: if there exists a polyon inscribed in one conic section and circumscribing another then it is part of an infinite family of such polygons.

Number Theory

Modular Arithmetic

Prime Factorization: unique decomposition in to representation $x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$

Greatest Common Divisor (GCD): product of minimum prime exponents.

Least Common Multiple (LCM): product of maximum prime exponents.

$ab = \text{GCD}(a,b) \cdot \text{LCM}(a,b)$ e.g.

Chinese Remainder: unique solution to system of coprime modular congruences.

Divisors: $n = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ has $(a_1+1)(a_2+1)\dots(a_n+1)$ divisors with sum $(1+p_1+\dots+p_1^{a_1})(1+p_2+\dots+p_2^{a_2})\dots(1+p_n+\dots+p_n^{a_n}) = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdot \dots \cdot \frac{p_n^{a_n+1}-1}{p_n-1}$

Phi Function: number of smaller coprime positive integers $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right) = n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\dots\left(\frac{p_n-1}{p_n}\right)$

Euler: $a^{\phi(n)} \equiv 1 \pmod{n}$

Wilson: $(p-1)! \equiv -1 \pmod{p}$ if and only if prime.

Pell: $x^2 - ny^2 = 1$ for positive non square n has infinitely many solutions. $(1,0), (x_1,y_1)$ and $x_k + y_k\sqrt{n} = (x_1 + y_1\sqrt{n})^k$ Fundamental Solution

There exist infinitely many triples (a,b,c) of positive integers such that a,b,c are in arithmetic progression and $ab+1, bc+1, ca+1$ are perfect squares. Proof: For (r,s) one of the infinitely many solutions to $x^2 - 3y^2 = 1$ consider $(2s-r, 2s, 2s+r)$

Euclid: $\text{GCD}(a,b) = ac + bd$ for some $c,d \in \mathbb{Z}$

Polignac v_p Of Factorial: $v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$

Sylvester: coprime a, b the greatest integer which is not a non negative integer linear combination of a and b is $ab-a-b$ and there are $\frac{(a-1)(b-1)}{2}$ such inexpressible.

Fibonacci: $1,1,2,3,5,8,13,21,34,55,89,144,\dots$ i.e. $F_n = F_{n-1} + F_{n-2}$ i.e. $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ i.e. $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ and by $1,2$ decompositions identities such as $F_{2n+1} = F_n^2 + F_{n+1}^2$, characteristic polynomial $x^2 - x - 1 = 0$ thus function $c_1 r_1^n + c_2 r_2^n + \dots$ in general constants and roots solve system of linear equations for constants, generating function $\sum_{n=1}^{\infty} F_n x^n = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \dots = \frac{x}{1-x-x^2}$

$F_{m+n+k} = F_{m+1}F_{n+1}F_{k+1} + F_m F_n F_k - F_{m-1}F_{n-1}F_{k-1}$

Zeckendorf: every positive integer can be uniquely written as a sum of distinct terms of the Fibonacci sequence, no 2 of which are consecutive.

Linear Recurrence Matrix:
$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n$ as
$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}^n = \begin{bmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{bmatrix}$ by induction
and directly from $M^{m+n} = M^mM^n$

Recursive system like the number of strings of length $n+1$ satisfying some desideratum which terminate in 0 or 1 based only on these numbers for the n case then matrix exponentiation works.

$u_{n+1} = 3u_n + 2v_n, v_{n+1} = u_n + v_n$
$\begin{bmatrix}u_{n+1}\\ v_{n+1}\end{bmatrix} = \begin{bmatrix}3 & 2\\ 1 & 1\end{bmatrix}\begin{bmatrix}u_n\\ v_n\end{bmatrix}$
$\begin{vmatrix}\lambda - 3 & -2\\ -1 & \lambda - 1\end{vmatrix}$
$\lambda_{1,2} = 2 \pm \sqrt{3} \to u_1 = 3, u_2 = 11 \to$
$u_n = \frac{1}{2\sqrt{3}}((\sqrt{3}+1)(2+\sqrt{3})^m + (\sqrt{3} - 1)(2-\sqrt{3})^m)$

Dirichlet: for coprime a, b there are infinitely many primes in the arithmetic progression $a, a+b, a+2b, \ldots$

Fermat 2 Square: every odd prime $p \equiv 1 \pmod 4$ can be expressed as the sum of 2 squares.

Lagrange 4 Square: every natural number can be expressed as the sum of 4 squares.

Wiefrich 9 Cube: every natural number can be expressed as the sum of 9 natural cubes.

Balasubramanian 19 Quarts: every natural number can be expressed as the sum of 19 natural quarts.

Waring-Hilbert: for every n there is a number $w(n)$ such that every natural is the sum of $w(n)$ natural nth powers.

Prime Number Theorem: the number of primes $\leq n$: $\pi(n) \sim \frac{n}{\log(n)}$

Quadratic Residue: nonzero $a \equiv b^2 \pmod p$ i.e. $\left(\frac{a}{p}\right) = 1$ else -1
$\left(\frac{a}{p}\right) = \left(\frac{a \pmod p}{p}\right)$
$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
Inspection And
Quadratic Reciprocity:
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Unique Inverse In $\mathbb{Z}/p\mathbb{Z}$
$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} \equiv$
$1 + 2 + \cdots + (p-1) \equiv \frac{p(p-1)}{2} \equiv 0 \pmod p$

Roots Of Unity Filter: e.g.
$\frac{1}{3}(1^n + w^n + w^{2n})$

Wolstenholme:
$p > 3$, $(p-1)!\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1}\right) \equiv 0 \pmod{p^2}$
$\binom{2p}{p} \equiv \binom{2}{1} \equiv 2 \pmod{p^3}$, $\binom{2p^n}{p^n} \equiv \binom{2p^{n-1}}{p^{n-1}} \pmod{p^{3n}}$

Lucas: $\binom{m}{n} \equiv \prod_{i=0}^{k}\binom{m_i}{n_i} \pmod p$ where $m = m_kp^k + m_{k-1}p^{k-1} + \cdots + m_1p + m_0, n = n_kp^k + n_{k-1}p^{k-1} + \cdots + n_1p + n_0$ are the base p expansions of m, n

Kummer: $v_p\left(\binom{a}{b}\right)$ is equal to the number of carries when b is added to $a-b$ in base p

Beatty: Let a and b be 2 positive

irrational numbers satisfying $\frac{1}{a} + \frac{1}{b} = 1$. Then the sequences $\lfloor an \rfloor$ and $\lfloor bn \rfloor$, $n \geq 1$, are strictly increasing and determine a partition of the set of positive integers in to 2 disjoint sets.

Newcomb: For exponential integral distribution the fraction with first digit n is $\log_{10}(n+1) - \log_{10}(n)$

Natural to reduce $(x^3 + y + 1)^2 + z^9$ modulo $2 \cdot 9 + 1 = 18 + 1 = 19$ because $a^{18} \equiv 1, 0 \pmod{19}$ and thus e.g. $z^9 \equiv \pm 1, 0 \pmod{19}$ as an nth degree polynomial (in this case $(z^9)^2 \equiv 1 \pmod{19}$) in a field such as $\mathbb{Z}/p\mathbb{Z}$ has n roots including multiplicities.

Pythagorean: Any solution x, y, z to the equation $x^2 + y^2 = z^2$ in positive integers is of the form with $u > v$ coprime and 1 even 1 odd $k[u^2 - v^2, 2uv, u^2 + v^2]$

Lifting The Exponent: if prime $p \nmid x, y$ then:
p is odd:
if $p|(x - y)$ then
$v_p(x^n - y^n) = v_p(x - y) + v_p(n)$
if n is odd and $p|(x + y)$ then
$v_p(x^n + y^n) = v_p(x + y) + v_p(n)$
$p = 2$:
if $4|(x - y)$ then
$v_2(x^n - y^n) = v_2(x - y) + v_2(n)$
if $2|(x - y)$ and n is even then
$v_2(x^n - y^n) =$
$v_2(x - y) + v_2(x + y) + v_2(n) - 1$
for all $p \nmid n$:
if $p|(x - y)$ then $v_p(x^n - y^n) = v_p(x - y)$
if $p|(x + y)$ and n is odd then
$v_p(x^n + y^n) = v_p(x + y)$

Let A be the set of all integers n such that $1 \leq n \leq 2021$ and $\gcd(n, 2021) = 1$. For every nonnegative integer j, let $S(j) = \sum_{n \in A} n^j$. Determine all values of j such that $S(j)$ is a multiple of 2021.

Linear Algebra

Length/Norm/Magnitude: $\begin{bmatrix} a_1 \\ a_2 \\ \cdots \\ a_n \end{bmatrix}$ is

$||a|| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$

Normalise To Unit: $\left(\frac{1}{||x||}\right) x$

Dot Product: $a \cdot b = ab^T = ||a||||b|| \cos(\theta) = a_1b_1 + a_2b_2 + \cdots + a_nb_n$

Orthogonal: if and only if $x \cdot y = 0$ i.e. 0 or $\theta = \frac{\pi}{2}$

Cauchy-Schwarz Inequality Discrete: $|x \cdot y| \leq (||x||)(||y||)$

Triangle Inequality: $||x + y|| \leq ||x|| + ||y||$

Projection Of b On To a: $\text{proj}_a b = p = \left(\frac{a \cdot b}{||a||^2}\right) a$

Diagonal, Identity, Upper Triangular, Lower Triangular, Symmetric (across diagonal) $A = A^T$, Skew-Symmetric (negative across diagonal) $A = -A^T$, Block Submatrices Decomposition

Every square matrix A can be decomposed uniquely as the sum of 2 matrices S and V where S is symmetric and V is skew-symmetric e.g. by taking the average of pairs for the symmetric and then the errors for the skew-symmetric.

$(AB)^T = B^T A^T$

Rank: the dimension of the vector space spanned by rows/columns.

Trace: of a square matrix, sum of elements on main diagonal and sum of eigenvalues (with multiplicity).

$\text{tr}(AB) = \text{tr}(BA)$

Idempotent: $A^2 = A$ e.g. $A^n = A$, diagonalizable and eigenvalues are 0 or 1

Gaussian Elimination

Row Operations

1: multiplying a row by a nonzero scalar e.g. multiplies determinant by that scalar.

2: adding a scalar multiple of a row to another row e.g. does not alter the determinant.

3: switching the positions of 2 rows in the matrix e.g. multiplies determinant by -1

In Gaussian elimination norm a leading nonzero entry to 1 and zero out in rows below until simple resolution of system of linear equations in terms of desired independent variables.

Application: Curve Fitting: rather than direct Lagrange Interpolation one can directly apply.

Gauss-Jordan Method (row reduction): norm to 1 as in Gaussian elimination and zeroes out rows below and rows above if possible so that non pivot

columns are independent.

Reduced Row Echelon Form RREF: the first nonzero entry in each row is 1, each successive row has its first nonzero entry in a later column, all entries above and below the first nonzero entry of each row are zero, all full rows of zeroes are the final rows of the matrix.

Homogeneous System: $AX = 0$ system of linear equations has a nontrivial number of solutions if and only if the RREF of A has fewer than n nonzero pivot entries.

Equivalent Systems: if and only if exactly the same solution set i.e. same RREF.

Row Space: the subset of $\mathbb{R}^n$ consisting of all vectors that are linear combinations of the rows of A

Inverse: $AB = BA = I$

$(AB)^{-1} = B^{-1}A^{-1}$

$(A^T)^{-1} = (A^{-1})^T$

Noninvertible: determinant is 0, rows/columns linearly dependent e.g. there exists non trivial linear combination to 0

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Inverse Method: convert $[A, I]$ in to RREF invertible if and only if $[I, A^{-1}]$

System Of Square Of Linear Equations: $AX = B$ has unique solution $A^{-1}B$ if and only if A is invertible else 0 or family of infinitely many.

Determinant: volume of paralleliped, product of eigenvalues (with multiplicity).

$\det(A) = \sum (\operatorname{sgn}(\sigma) \prod a_{i,\sigma_i})$

The usual row minors expansion identifying with torus.

Cauchy-Binet: $\det(AB) = \sum_{S \in \binom{[n]}{m}} \det(A_{[m],S}) \det(B_{S,[m]})$

Vandermonde:
$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{i<j}(x_j - x_i)$$

Strictly Diagonally Dominant: invertible if $|a_{ii}| > \sum_{j \neq i} |a_{ij}|$ for all i

Cramer: $AX = B, |A| \neq 0$ let A_i be A with the ith column replaced by B then the entries of the unique solution $X = A^{-1}B$ are $x_i = \frac{|A_i|}{|A|}$

Eigenvalue And Eigenvector: $AX = \lambda X$ i.e. eigenvalue λ corresponding with eigenvector X solution of $(\lambda I - A)X = 0$

Eigenspace: the set of eigenvectors corresponding with λ e.g.

Characteristic Polynomial Of A Matrix: $p_A(x) = |xI - A|$ for example as $AX = \lambda X \to (\lambda I - A)X = 0$ and the eigenvalues are the roots (real) then one can resolve the homogeneous system,

i.e. Vieta's sum of eigenvalues/trace and determinant (for $x = 0$)

Eigenvalues Of Symmetric Matrices Are Real
Eigenvectors Of Distinct Eigenvalues Are Orthogonal
Correlation And Covariance Matrices Positive Semidefinite: all eigenvalues are nonnegative, all upper left or lower right matrices have nonnegative determinants, $x^T Ax \geq 0 \forall x$

Spectral Mapping: Let A be an $n \times n$ matrix with not necessarily distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ and let $P(x)$ be a polynomial. Then the eigenvalues of the matrix $P(A)$ are $P(\lambda_1), P(\lambda_2), \ldots, P(\lambda_n)$

Cayley-Hamilton: A satisfies its own characteristic polynomial.

2×2 matrices
$A^2 - \text{tr}(A) \cdot A + \det(A) \cdot I = 0$

Perron-Frobenius: Any square matrix with positive entries has a unique eigenvector with positive entries (up to multiplication by a positive scalar), and the corresponding eigenvalue has multiplicity 1 and is strictly greater than the absolute value of any other eigenvalue.

Similar: if there exists invertible P such that $P^{-1}AP = B$, identical characteristic polynomials check diagonal similar.

Diagonal Similar: the ith column of P is an eigenvector for A then if P is invertible we obtain $D = P^{-1}AP$ is diagonal with eigenvalues on diagonal.

$A^k = PD^kP^{-1}$

Recall that $X(t)$ has column vectors from the free components in the general solution to an ODE whence
$e^{At} = X(t)(X(0))^{-1}$

$1 + X + X^2 + \cdots = (1 - X)^{-1}$ as in reals and similar.

Diagonalization Method

1 Characteristic polynomial
$p_A(x) = |xI - A|$
2 Find all real roots of $p_A(x)$ are eigenvalues λ_i
3 For each eigenvalue row reduce $[\lambda_i I - A|0]$ and obtain a set of particular solutions of the homogeneous system $(\lambda_i I - A)x = 0$ by setting each independent variable in turn to 1 and all other independent variables to 0
4 If and only if one obtains n fundamental eigenvectors can A be diagonalised.
5 Form a matrix P whose columns are these n fundamental eigenvectors.
6 $D = P^{-1}AP$ is a diagonal matrix whose d_{ii} entry is the eigenvalue for the fundamental eigenvector forming the ith column of P and note that $A = PDP^{-1}$

Translation: add.

Dilations: multiply by scalar.

Reflection: $\begin{bmatrix}\cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta)\end{bmatrix}$

Rotation: $\begin{bmatrix}\cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta)\end{bmatrix}$

Kernel/Nullspace: $\ker(L)$ is the subset of all vectors in V that map to 0_W

From RREF produce in terms of independent variables and then form basis e.g. by subtituting in dummy variables.

Range: $\text{range}(L)$ is the subset of all vectors in W that are the image of some vector in V

From RREF take other nonzero pivot columns corresponding in A as a basis for $\text{range}(L)$

$\dim(\text{range}(L)) = \text{rank}(A)$

$\dim(\ker(L)) = n - \text{rank}(A)$

$\dim(\ker(L)) + \dim(\text{range}(L)) = n$

Dimension Theorem:
$\dim(\ker(L)) + \dim(\text{range}(L)) = \dim(V)$

Transition Matrix Change Of Basis:
$X_{\text{old}} = AX_{\text{new}}$ in terms of coordinates under these bases.

Nilpotent Matrix: A if there exists index/degree k such that $A^k = 0$

Nilpotent if and only if for all $k > 0$, $\text{tr}(A^k) = 0$

Orthogonal Matrix: $A^{-1} = A^T$

Hermitian Matrix: $A = A^*$ complex conjugate transpose.

Unitary Matrix: $A^{-1} = A^*$

Orthogonal Set Of Vectors: pairwise orthogonal i.e. dot product 0

Orthonormal Set Of Vectors:
orthogonal set of unit vectors.

v is represented
$(v \cdot v_1)v_1 + (v \cdot v_2)v_2 + \cdots + (v \cdot v_k)v_k$ for ordererd orthornormal basis
$B = (v_1, v_2, \ldots, v_k)$

Gram-Schmidt Process: Finding An Orthogonal Basis For A Subspace Of $\mathbb{R}^n$

Given linearly independent $w_1, w_2, \ldots, w_k$ of $\mathbb{R}^n$ an orthogonal basis for the span is:

$v_1 = w_1$

$v_2 = w_2 - \left(\frac{w_2 \cdot v_1}{v_1 \cdot v_1}\right) v_1$

$v_3 = w_3 - \left(\frac{w_3 \cdot v_1}{v_1 \cdot v_1}\right) v_1 - \left(\frac{w_3 \cdot v_2}{v_2 \cdot v_2}\right) v_2$

$\ldots$

Any orthogonal set of nonzero vectors in W is contained in an orthogonal basis for W

Orthogonal Matrix: $A^T = A^{-1}$

If A and B are orthogonal matrices then $|A| = \pm 1$, $A^T = A^{-1}$ is orthogonal, AB is orthogonal.

A is orthogonal if and only if its rows/columns form an orthornomal basis for $\mathbb{R}^n$

If B and C are ordered orthonormal bases then the transition is an orthogonal matrix.

If A is orthogonal then $v \cdot w = Av \cdot Aw$

Orthogonal Complement: $W^\perp$ of W is the set of all vectors $x \in \mathbb{R}^n$ with the property that $x \cdot w$ for all $w \in W$

$v \in W^\perp$ if and only if v is orthogonal to every vector in a spanning set for W

Projection Theorem: every vector v can be expressed uniquely as $w_1 + w_2$ where $w_1 \in W$ and $w_2 \in W^\perp$

Orthogonal Projection: if W is a subspace with orthonormal basis $u_1, u_2, \ldots, u_k$ then the orthogonal projection is $(v \cdot u_1)u_1 + (v \cdot u_2)u_2 + \cdots + (v \cdot u_k)u_k$

$v = \text{proj}_W v + v - \text{proj}_W v = \text{proj}_W v + \text{proj}_{W^\perp} v$

The projection is the closest point in W to P

Orthogonal Diagonalization: linear operators have an orthonormal basis B of eigenvectors said to be orthogonally diagonalizable, the transition matrix from B-coordinates to standard coordinates is an orthogonal matrix.

Symmetric Operator: let V be a subspace of $\mathbb{R}^n$ a linear operator $L : V \to V$ is a symmetric operator on V if and only if $L(v_1) \cdot v_2 = v_1 \cdot L(v_2)$ for every $v_1, v_2 \in V$

Symmetric operator L on a nontrivial subspace of $\mathbb{R}^n$ has at least 1 real eigenvalue.

Complex Dot Product: $z \cdot w = z_1\overline{w_1} + z_2\overline{w_2} + \cdots + z_n\overline{w_n}$

Conjugate Transpose: $Z^* = \left(\overline{Z}\right)^T$

Hermitian Matrix: $A = A^*$ complex conjugate transpose.

Skew-Hermitian Matrix: $-A = A^*$

Normal Matrix: $AA^* = A^*A$

Unitary Matrix: $A^{-1} = A^*$

All eigenvalues of a Hermitian matrix are real.

The total number of paths from P_i to P_j of length k is given by the (i, j) entry in the matrix A^k where A is the adjacency matrix.

The total number of paths of length $\leq k$ from a vertex P_i to P_j is the (i, j) entry of $A + A^2 + \cdots + A^k$ and of course $(A + A^2 + \cdots + A^k)(I - A) = A - A^{k+1}$ whence one obtains $(A - A^{k+1})(I - A)^{-1}$ e.g.

Jordan Normal/Canonical Form: e.g.
$$\begin{bmatrix} \lambda_1 & 1 & 0 & 0 & 0 \\ 0 & \lambda_1 & 1 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & \lambda_2 & 1 \\ 0 & 0 & 0 & 0 & \lambda_2 \end{bmatrix}$$

Hadamard: an $n \times n$ matrix with ± 1 entries has absolute determinant at most $n^{\frac{n}{2}}$ with equality if and only if the

rows are mutually orthogonal.

Lindsey: the sum of the entries in any $a \times b$ submatrix of a Hadamard matrix is at most $\sqrt{abn}$

QR Decomposition: for each invertible matrix A, there is a unique pair of orthogonal matrix Q and upper-triangular matrix R with positive diagonal elements such that $A = QR$. QR Decomposition is often used to solve linear systems $Ax = b$ when A is an invertible matrix. Since Q is an orthogonal matrix, $Q^{-1} = Q^T$ and $QRx = b \to Rx = Q^T b$. Because R is an upper-triangular matrix, we can begin with x_n and recursively calculate all $x_i, \forall i = n, n-1, \ldots, 1$.

Example: the linear least squares regression $(X^T X)\hat{\beta} = X^T Y$.

LU Decomposition: for each invertible matrix A, expresses A as a product of a lower and upper triangular matrix $A = LU$. LU decomposition can be used to solve $Ax = b$ and calculate the determinant of A.
$LUx = b \to Ly = b, Ux = y$ and
$\det(A) = \det(L)\det(U) = \prod L_{i,i} \prod U_{i,i}$

Cholesky Decomposition: when A is a symmetric positive definite matrix, expresses $A = R^T R$ where R is a unique upper triangular matrix with positive diagonal entries. Essentially, it is a LU decomposition with the property $L = U^T$.

Example: to generate correlated random variables that follow a n-dimensional multivariate normal distribution
$X = [X_1, X_2, \ldots, X_n]^T \sim N(\mu, \Sigma)$ with mean $\mu = [\mu_1, \mu_2, \ldots, \mu_n]^T$ and covariance matrix Σ [a $n \times n$ positive definite matrix], we can decompose the covariance matrix Σ into $R^T R$ and then X can be generated as $X = \mu + R^T Z$.

Abstract Algebra

Group: set G with binary operation $a \cdot b = ab$
1 Associativity: $(ab)c = a(bc)$ for all $a, b, c \in G$.
2 Identity: there exists unique identity e such that $ae = ea = a$ for all $a \in G$.
3 Inverses: for each $a \in G$ there exists unique inverse $b \in G$ such that $ab = ba = e$.

Z_n: addition modulo n.

D_n: dihedral group, rotations and reflections.

$U(n), G_n$: multiplication of coprime residues modulo n.

Sym(X): symmetry group of object X, transformations under which the object is invariant, under the operation of composition.

Aut(G): the group of automorphisms on the group G.

Permutation Group: a group whose elements are permutations of a given set M and whose group operation is the composition of permutations.

S_n Symmetric Group On n Letters: the group of all permutations on $\{1, 2, \ldots, n\}$.

$GL(n, F)$ General Linear Group: the set of $n \times n$ invertible matrices with entries from F with matrix multiplication as the group operation.

$SL(n, F)$ Special Linear Group: the subgroup of $GL(n, F)$ consisting of matrices with determinant 1.

Abelian: $ab = ba$ for all $a, b \in G$.

Cancellation:
$ba = ca \rightarrow baa^{-1} = caa^{-1} \rightarrow b = c$.

Order Of A Group: the number of elements of a group denoted $|G|$.

Order Of An Element: smallest positive integer n such that $a^n = e$ denoted $|a|$ can be infinite.

Subgroup: if a subset H of a group G is itself a group under the operation of G we say that H is a subgroup of G denoted $H \leq G$, proper (non-G) subgroup $H < G$ and trivial subgroup $\{e\}$.

Subgroup Criterion: if H is a nonempty subset of G and $ab^{-1} \in H$ for all $a, b \in H$, then H is a subgroup of G.

Subgroup Criteria: if H is a nonempty subset of G and $ab, a^{-1} \in H$ for all $a, b \in H$, then H is a subgroup of G.

Not A Subgroup:.
1 Show that the identity is not in the set.
2 Exhibit an element of the set whose inverse is not in the set.
3 Exhibit 2 elements of the set whose product is not in the set.

Finite Subgroup Criterion: if H is a nonempty finite subset of a group G and H is closed under the operation of

G then H is a subgroup of G.

Cyclic Subgroup Of G Generated By a: $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

Center Of A Group: the center $Z(G)$ is the subset of elements in G that commute with every element of G i.e. $Z(G) = \{a \in G | ab = ba \text{ for all } b \in G\}$.

Center Is A Subgroup.

Centraliser Of a In G: for a fixed element $a \in G$ the centraliser of a in G, $C(a)$ is the set of all elements in G that commute with a, $C(a) = \{b \in G | ab = ba\}$.

Cyclic Group: if there exists a generator element $a \in G$ such that $G = \{a^n | n \in \mathbb{Z}\}$.

Criterion For $a^i = a^j$: if a has infinite order then $a^i = a^j$ if and only if $i = j$. If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

$|a| = |\langle a \rangle|$.

$a^k = e$ Implies That $|a|$ Divides k.

$\langle a^k \rangle = \langle a^{\text{GCD}(n,k)} \rangle$.

Criterion For $\langle a^i \rangle = \langle a^j \rangle$ And $|a^i| = |a^j|$: let $|a| = n$ then if and only if $\text{GCD}(n, i) = \text{GCD}(n, j)$.

Generator Of Finite Cyclic Groups: let $|a| = n$ then $\langle a \rangle = \langle a^j \rangle$ and $|a| = |\langle a^j \rangle|$ if and only if $\text{GCD}(n, j) = 1$.

Generators Of Z_n: an integer k in Z_n is a generator of Z_n if and only if $\text{GCD}(n, k) = 1$.

Fundamental Theorem Of Cyclic Groups: every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$ then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly 1 subgroup of order k - namely, $\langle a^{n/k} \rangle$.

Number Of Elements Of Each Order In A Cyclic Group: if d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Number Of Elements Of Order d In A Finite Group: in a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Permutation Of A: a function from a set A to A that is both one-to-one and onto.

Permutation Group Of A: a set of permutations of A that forms a group under function composition.

Products Of Disjoint Cycles: every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Disjoint Cycles Commute: if the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Order Of A Permutation: the order of a permutation of a finite set written in

disjoint cycle form is the least common multiple of the lengths of the cycles.

Product Of 2-Cycles: every permutation in S_n, $n > 1$, is a product of 2-cycles.

If $e = \beta_1\beta_2 \dots \beta_r$, where the β's are 2-cycles, then r is even.

Always Even Or Always Odd: if a permutation α can be expressed as a product of an even/odd number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even/odd number of 2-cycles.

Even Permutations Form A Group: the set of even permutations in S_n forms a subgroup of S_n.

Alternating Group Of Degree n: the group of even permutations of n symbols is denoted by A_n and is called the alternating group of degree n.

For $n > 1$, A_n has order $\frac{n!}{2}$.

Group Isomorphism: an isomorphism ϕ from a group G to a group $\bar{G}$ is a one-to-one mapping (or function) from G onto $\bar{G}$ that preserves the group operation. That is, $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. If there is an isomorphism from G onto $\bar{G}$, we say that G and $\bar{G}$ are isomorphic and write $G \approx \bar{G}$.

Cayley: every group is isomorphic to a group of permutations.

Properties Of Isomorphisms Acting On Elements: suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then.
1 ϕ carries the identity of G to the identity of $\bar{G}$.
2 for every integer n and for every group element $a \in G$, $\phi(a^n) = (\phi(a))^n$
3 for any elements $a, b \in G$, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute
4 $G = \langle a \rangle$ if and only if $\bar{G} = \langle \phi(a) \rangle$
5 $|a| = |\phi(a)|$ for all $a \in G$ (isomorphisms preserve orders)
6 for a fixed integer k and a fixed group element $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\bar{G}$.
7 if G is finite, then G and $\bar{G}$ have exactly the same number of elements of every order.

Properties Of Isomorphisms Acting On Groups: suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then.
1 ϕ^{-1} is an isomorphism from $\bar{G}$ onto G.
2 G is Abelian if and only if $\bar{G}$ is Abelian.
3 G is cyclic if and only if $\bar{G}$ is cyclic.
4 if K is a subgroup of G, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of $\bar{G}$
5 if $\bar{K}$ is a subgroup of $\bar{G}$ then $\phi^{-1}(\bar{K}) = \{g \in G | \phi(g) \in \bar{K}\}$ is a subgroup of G.
6 $\phi(Z(G)) = Z(\bar{G})$.

Automorphism: an isomorphism from a group G onto itself is called an automorphism of G.

Inner Automorphism Induced By a: let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all $x \in G$ is called the inner automorphism of G induced by a.

Aut(G): the set of all automorphisms of G.

Inn(G): the set of all inner automorphisms of G.

Aut(G) And Inn(G) Are Groups: the set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

Aut(Z_n) $\approx U(n)$: for every positive integer n, Aut(Z_n) is isomorphic to $U(n)$.

Coset Of H In G: let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah | h \in H\}$ is denoted by aH. Analagously, $Ha = \{ha | h \in H\}$ and $aHa^{-1} = \{aha^{-1} | h \in H\}$. When H is a subgroup of G, the set aH is called the left coset of H in G containing a, whereas Ha is called the right coset of H in G containing a. In this case, the element a is called the coset representative of aH (or Ha). We use $|aH|$ to denote the number of elements in the aH, and $|Ha|$ to denote the number of elements in Ha.

Properties Of Cosets: let H be a subgroup of G, and let $a, b \in G$. Then.
1 $a \in aH$.
2 $aH = H$ if and only if $a \in H$.
3 $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
4 $aH = bH$ if and only if $a \in bH$.
5 $aH = bH$ or $aH \cap bH = \varnothing$.
6 $aH = bH$ if and only if $a^{-1}b \in H$.
7 $|aH| = |bH|$.
8 $aH = Ha$ if and only if $H = aHa^{-1}$.
9 aH is a subgroup of G if and only if $a \in H$.

Lagrange: $|H|$ Divides $|G|$: if G is a finite group and H is a subgroup of G, then H divides G. Moreover, the number of distinct left (right) cosets of H in G is $\frac{|G|}{|H|}$.

$|G : H| = \frac{|G|}{|H|}$: if G is a finite group and H is a subgroup of G, then $|G : H| = \frac{|G|}{|H|}$.

$|a|$ Divides $|G|$: in a finite group, the order of each element of the group divides the order of the group.

Groups Of Prime Order Are Cyclic: a group of prime order is cyclic.

$a^{|G|} = e$: let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.

$|HK| = \frac{|H||K|}{|H \cap K|}$: for 2 finite subgroups H and K of a group, define the set $HK = \{hk | h \in H, k \in K\}$. Then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Classification Of Groups Of Order $2p$: let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to Z_{2p} or D_p.

Stabiliser Of A Point: let G be a group of permutations of a set S. For each i in S, let $\text{stab}_G(i) = \{\phi \in G | \phi(i) = i\}$. We call $\text{stab}_G(i)$ the stabiliser of i in G.

Orbit Of A Point: let G be a group of permutations of a set S. For each i in S, let $\text{orb}_G(i) = \{\phi(i) | \phi \in G\}$. The set $\text{orb}_G(i)$ is a subset of S called the orbit of i under G. We use $|\text{orb}_G(i)|$ to denote the number of elements in $\text{orb}_G(i)$.

Orbit-Stabiliser Theorem: let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |\text{orb}_G(i)||\text{stab}_G(i)|$.

The Rotation Group Of A Cube: the group of rotations of a cube is isomorphic to S_4.

External Direct Product: let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

Order Of An Element In A Direct Product: the order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. $|(g_1, g_2, \ldots, g_n)| = \text{LCM}(|g_1|, |g_2|, \ldots, |g_n|)$.

Criterion For $G \oplus H$ To Be Cyclic: let G and H be finite cyclic group. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are coprime.

Criterion For $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ To Be Cyclic: an external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ are pairwise coprime.

Criterion For $Z_{n_1 n_2 \ldots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$: let $m = n_1 n_2 \ldots n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ of and only if n_i are pairwise coprime.

$U(n)$ As An External Direct Product: suppose s and t are coprime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short, $U(st) \approx U(s) \oplus U(t)$. Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$.

Normal Subgroup: a subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. We denote this by $H \lhd G$.

Normal Subgroup Test: a subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all $x \in G$.

Factor Groups: let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH | a \in G\}$ is a group under the operation $(aH)(bH) = abH$.

G/Z: let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

$G/Z(G) \approx \text{Inn}(G)$: for any group G, $G/Z(G)$ is isomorphic to $\text{Inn}(G)$.

Cauchy For Abelian Groups: let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

Internal Direct Product Of H And K: we say that G is the internal direct product of H and K and write $G = H \times K$ if H and K are normal subgroups of G and $G = HK$ and $H \cap K = \{e\}$.

Internal Direct Product $H_1 \times H_2 \times \cdots \times H_n$: let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the internal direct product of $H_1, H_2, \ldots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if.
1 $G = H_1H_2 \ldots H_n = \{h_1h_2 \ldots h_n | h_i \in H_i\}$.
2 $(H_1H_2 \ldots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \ldots, n-1$.

$H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$: if a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2, \ldots, H_n$.

Classification Of Groups Of Order p^2: every group of order p^2, where p is a prime, is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$.

If G is a group of order p^2, where p is a prime, then G is Abelian.

Group Homomorphism: a homomorphism ϕ from a group G to a group $\bar{G}$ is a mapping from G into $\bar{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Kernel Of A Homomorphism: the kernel of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G | \phi(x) = e\}$. The kernel of ϕ is denoted by Ker ϕ.

Properties Of Elements Under Homomorphisms: let ϕ be a homomorphism from a group G to a group $\bar{G}$ and let g be an element of G. Then.
1 ϕ carries the identity of G to the identity of $\bar{G}$.
2 $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$.
3 if $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.
4 Ker ϕ is a subgroup of G.
5 $\phi(a) = \phi(b)$ if and only if a Ker $\phi = b$ Ker ϕ.
6 if $\phi(g) = g'$ then $\phi^{-1}(g') = \{x \in G | \phi(x) = g'\} = g$ Ker ϕ.

Properties Of Subgroups Under Homomorphism: let ϕ be a homomorphism from a group G to a group $\bar{G}$ and let H be a subgroup of G. Then.
1 $\phi(H) = \{\phi(h) | h \in H\}$ is a subgroup of $\bar{G}$.
2 if H is cyclic then $\phi(H)$ is cyclic.
3 if H is Abelian then $\phi(H)$ is Abelian.
4 if H is normal in G then $\phi(H)$ is normal in $\phi(G)$.
5 if $|\text{Ker } \phi| = n$ then ϕ is an n-to-1

mapping from G onto $\phi(G)$.
6 if $|H| = n$ then $|\phi(H)|$ divides n.
7 if $\bar{K}$ is a subgroup of $\bar{G}$ then $\phi^{-1}(\bar{K}) = \{k \in G | \phi(k) \in \bar{K}\}$ is a subgroup of G.
8 if $\bar{K}$ is a normal subgroup of $\bar{G}$ then $\phi^{-1}(\bar{K}) = \{k \in G | \phi(k) \in \bar{K}\}$.
9 if ϕ is onto and Ker $\phi = \{e\}$ then ϕ is an isomorphism from G to $\bar{G}$.

Kernels Are Normal: let ϕ be a group homomorphism from G to $\bar{G}$. Then Ker ϕ is a normal subgroup of G.

First Isomorphism: let ϕ be a group homomorphism from G to $\bar{G}$. Then the mapping from $G/\text{Ker } \phi$ to $\phi(G)$, given by g Ker $\phi \to \phi(G)$, is an isomorphism. $G/\text{Ker } \phi \approx \phi(G)$.

If ϕ is a homomorphism from a finite group G to $\bar{G}$, then $|\phi(G)|$ divides $|G|$ and $|\bar{G}|$.

Normal Subgroups Are Kernels: every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.

Fundamental Theorem Of Finite Abelian Groups: every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Determining The Isomorphism Class Of G: for a finite Abelian group G, writing in the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_k^{n_k}}$ where the p_is are not necessarily distinct primes and the prime powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G.

Greedy Algorithm For An Abelian Group Of Order p^n:.
1 compute the orders of the elements of the group G.
2 select an element a_1 or maximum order and define $G_1 = \langle a_1 \rangle$. Set $i = 1$.
3 if $|G| = |G_i|$, stop. Otherwise, replace i by $i + 1$.
4 select an element a_i of maximum order p^k such that $p^k \leq \frac{|G|}{|G_{i-1}|}$ and none of $a_i, a_i^p, a_i^{p^2}, \ldots, a_i^{p^{k-1}}$ is in G_{i-1}, and define $G_i = G_{i-1} \times \langle a_i \rangle$.
5 return to step 3.

Existence Of Subgroups Of Abelian Groups: if m divides the order of a finite Abelian group G, then G has a subgroup of order m.

Ring: a ring R is a set with 2 binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:.
1 $a + b = b + a$.
2 $(a + b) + c = a + (b + c)$.
3 there is an additive identity 0. That is, there is an element 0 in R such that $a + 0 = a$ for all $a \in R$.
4 there is an element $-a \in R$ such that $a + (-a) = 0$.
5 $a(bc) = (ab)c$.
6 $a(b + c) = ab + ac$ and

$(b+c)a = ba + ca$.

Commutative Ring: e.g. $ab = ba$ for all $a, b \in R$.

Uniqueness Of The Unity And Inverses: if a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Subring: a subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

Subring Criterion: a nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication - that is, if $a - b$ and ab are in S whenever a and b are in S.

Unity/Identity: a nonzero element that is an identity under multiplication.

Unit: a nonzero element of a commutative ring with unity with a multiplicative inverse, a is a unit if a^{-1} exists.

If a and b belong to a commutative ring R and a is nonzero we say that a divides b (or that a is a factor of b) and write $a|b$, if there exists an element c in R such that $b = ac$. If a does not divide b, we write $a \nmid b$.

Zero-Divisors: a zero-divisor is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = ba = 0$.

Integral Domain: an integral domain is a commutative ring with unity and no zero-divisors.

Cancellation: let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Field: a field is a commutative ring with unity in which every nonzero element is a unit. It is often helpful to think of ab^{-1} as a divided by b. With this in mind, a field can be thought of as simply an algebraic system that is closed under addition, subtraction, multiplication, and division (except by 0).

Finite Integral Domains Are Fields: a finite integral domain is a field.

Z_p Is A Field: for every prime p, Z_p, the ring of integers modulo p is a field.

Characteristic Of A Ring: the characteristic of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.

Characteristic Of A Ring With Unity: let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

Characteristic Of An Integral Domain: the characteristic of an integral domain is 0 or prime.

Ideal: a subring A of a ring R is called a

(two-sided) ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A. So, a subring A of a ring R is an ideal of R if A absorbs elements from R.

Ideal Test: a nonempty subset A of a ring R is an ideal of R if.
1 $a - b \in A$ whenever $a, b \in A$.
2 ra and ar are in A whenever $a \in A$ and $r \in R$.

Principal Ideal Generated By a: let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra | r \in R\}$ is an ideal of R called the principal ideal generated by a.

Ideal Generated By $a_1, a_2, \ldots, a_n$: let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n$ belong to R. Then $I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \ldots r_na_n | r_i \in R\}$ is an ideal of R called the ideal generated by $a_1, a_2, \ldots, a_n$.

Existence Of Factor Rings: let R be a ring and let A be a subring of R. The set of cosets $\{r + A | r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

Prime Ideal, Maximal Ideal: a prime ideal A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A maximal ideal of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

R/A Is An Integral Domain If And Only If A Is Prime: let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

R/A Is A Field If And Only If A Is Maximal: let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

Ring Homomorphism, Ring Isomorphism: a ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the 2 ring operations; that is, for all $a, b \in R$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

Properties Of Ring Homomorphisms: let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.
1 for any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
2 $\phi(A) = \{\phi(a) | a \in A\}$ is a subring of S.
3 if A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.
4 $\phi^{-1}(B) = \{r \in R | \phi(r) \in B\}$ is an ideal of R.
5 if R is commutative, then $\phi(R)$ is commutative.
6 if R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.

7 ϕ is an isomorphism if and only if ϕ is onto and
Ker $\phi = \{r \in R | \phi(r) = 0\} = \{0\}$.
8 if ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

Kernels Are Ideals: let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker $\phi = \{r \in R | \phi(r) = 0\}$ is an ideal of R.

First Isomorphism Theorem For Rings: let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\text{Ker } \phi$ to $\phi(R)$, given by $r + \text{Ker } \phi \to \phi(r)$, is an isomorphism. In symbols,
$R/\text{Ker } \phi \approx \phi(R)$.

Ideals Are Kernels: every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A.

Homomorphism From Z To A Ring With Unity: let R be a ring with unity 1. The mapping $\phi : Z \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

A Ring With Unity Contains Z_n Or Z: if R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to Z_n. If the characteristic of R is 0, then R contains a subring isomorphic to Z.

Z_m Is A Homomorphic Image Of Z: for any positive integer m, the mapping of $\phi : Z \to Z_m$ given by $x \to x \pmod m$ is a ring homomorphism.

A Field Contains Z_p Or Q: if F is a field of characteristic p, then F contains a subfield isomorphic to Z_p. If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers.

Field Of Quotients: let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.

Ring Of Polynomials Over R: let R be a commutative ring. The set of formal symbols $R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, n \in \mathbb{Z}_{\geq 0}\}$ is called the ring of polynomials over R in the indeterminate x.

Addition And Multiplication In $R[x]$.

D An Integral Domain Implies $D[x]$ An Integral Domain: if D is an integral domain, then $D[x]$ is an integral domain.

Division Algorithm For $F[x]$: let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.

Remainder Theorem: let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Factor Theorem: let F be a field,

$a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Polynomials Of Degree n Have At Most n Zeros: a polynomial of degree n over a field has at most n zeros, counting multiplicity.

Principal Ideal Domain (PID): a principal ideal domain is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra | r \in R\}$ for some $a \in R$.

$F[x]$ Is A PID: let F be a field. Then $F[x]$ is a principal ideal domain.

Criterion For $I = \langle g(x) \rangle$: let F be a field, I a nonzero ideal in $F[x]$. and $g(x)$ an element of $F[x]$. Then $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

Irreducible Polynomial, Reducible Polynomial: let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called reducible over D.

Reducibility Test For Degrees 2 And 3: let F be a field. If $f(x) \in F[x]$ and deg $f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Content Of A Polynomial, Primitive Polynomial: the content of a nonzero polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, where the a_is are integers, is the GCD of the integers $a_n, a_{n-1}, \ldots, a_0$. A primitive polynomial is an element of $Z[x]$ with content 1.

Gauss's Lemma: the product of 2 primitive polynomials is primitive.

Reducibility Over Q Implies Reducibility Over Z: let $f(x) \in Z[x]$. If $f(x)$ is reducible over Q, then it is reducible over Z.

Mod p Irreducibility Test: let p be a prime and suppose that $f(x) \in Z[x]$ with deg $f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over Z_p and deg $\bar{f}(x) =$ deg $f(x)$, then $f(x)$ is irreducible over Q.

Eisenstein's Criterion: let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in Z[x]$. If there is a prime p such that $p \nmid a_n, p | a_{n-1}, \ldots, p | a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over Q.

Irreducibility Of pth Cyclotomic Polynomial: for any prime p, the pth cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over Q.

$\langle p(x) \rangle$ Is Maximal If And Only If $p(x)$ Is Irreducible: let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal

ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.

$F[x]/\langle p(x)\rangle$ Is A Field: let F be a field and $p(x)$ be an irreducible polynomial over F. Then $F[x]/\langle p(x)\rangle$ is a field.

$p(x)|a(x)b(x)$ Implies $p(x)|a(x)$ Or $p(x)|b(x)$: let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x)|a(x)b(x)$, then $p(x)|a(x)$ or $p(x)|b(x)$.

Unique Factorization In $Z[x]$: every polynomial in $Z[x]$ that is not the zero polynomial or a unit in $Z[x]$ can be written in the form $b_1 b_2 \dots b_s p_1(x) p_2(x) \dots p_m(x)$, where the b_is are irreducible polynomials of degree 0 and the $p_i(x)$s are irreducible polynomials of positive degree. Furthermore, if $b_1 b_2 \dots b_s p_1(x) p_2(x) \dots p_m(x) = c_1 c_2 \dots c_t q_1(x) q_2(x) \dots q_n(x)$, where the b_is and c_is are irreducible polynomials of degree 0 and the $p_i(x)$s and $q_i(x)$s are irreducible polynomials of positive degree, then $s = t, m = n$, and, after renumbering the cs and $q(x)$s, we have $b_i = \pm c_i$, for $i = 1, 2, \dots, s$ and $p_i(x) = \pm q_i(x)$ for $i = 1, 2, \dots, m$.

Associates, Irreducibles, Primes: elements a and b of an integral domain D are called associates if $a = ub$, where u is a unit of D. A nonzero elements a of an integral domain D is called an irreducible if a is not a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit. A nonzero element a of an integral domain D is called a prime if a is not a unit and $a|bc$ implies $a|b$ or $a|c$.

Prime Implies Irreducible: in an integral domain, every prime is an irreducible.

PID Implies Irreducible Equals Prime: in a principal ideal domain, an element is an irreducible if and only if it is a prime.

Unique Factorization Domain (UFD): an integral domain D is a unique factorization domain if.
1 every nonzero element of D that is not a unit can be written as a product of irreducibles of D; and.
2 the factorization into irreducibles is unique up to associates and the order in which the factors appear.

PID Implies UFD: every principal ideal domain is a unique factorization domain.

$F[x]$ Is A UFD: let F be a field. Then $F[x]$ is a unique factorization domain.

Euclidean Domain (ED): an integral domain D is called a Euclidean domain if there is a function d (called the measure) from the nonzero elements of D to the non negative integers such that.
1 $d(a) \leq d(ab)$ for all nonzero $a, b \in D$; and.
2 if $a, b \in D, b \neq 0$, then there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

ED Implies PID: every Euclidean

domain is a principal ideal domain.

ED Implies UFD: every Euclidean domain is a unique factorization domain.

D A UFD Implies $D[x]$ A UFD: if D is a unique factorization domain, then $D[x]$ is a unique factorization domain.

Vector Space: a set V is said to be a vector space over a field F if V is an Abelian group under addition (denoted by $+$) and, if for each $a \in F$ and $v \in V$, there is an element av in V such that the following conditions hold for all $a, b \in F$ and all $u, v \in V$.
1 $a(v + u) = av + au$.
2 $(a + b)v = av + bv$.
3 $a(bv) = (ab)v$.
4 $1v = v$.

Subspace: let V be a vector space over a field F and let U be a subset of V. We say that U is a subspace of V if U is also a vector space over F under the operations of V.

Linearly Dependent, Linearly Independent: a set S of vectors is said to be linearly dependent over the field F if there are vectors $v_1, v_2, \ldots, v_n$ from S and elements $a_1, a_2, \ldots, a_n$ from F, not all zero, such that $a_1v_1 + a_2v_2 + \ldots a_nv_n = 0$. A set of vectors that is not linearly dependent over F is called linearly independent over F.

Basis: let V be a vector space over F. A subset B of V is called a basis for V if B is linearly independent over F and every element of V is a linear combination of elements of B.

Invariance Of Basis Size: if $\{u_1, u_2, \ldots u_m\}$ and $\{w_1, w_2, \ldots, w_n\}$ are both bases of a vector space V over a field F, then $m = n$.

Dimension: a vector space that has a basis consisting of n elements is said to have dimension n. For completeness, the trivial vector space $\{0\}$ is said to be spanned by the empty set and to have dimension 0.

Extension Field: a field E is an extension field of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F.

Fundamental Theorem Of Field Theory: let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.

Splitting Field: let E be an extension field of F and let $f(x) \in F[x]$ with degree at least 1. We say that $f(x)$ splits in E if there are elements $a \in F$ and $a_1, a_2, \ldots, a_n \in E$ such that $f(x) = a(x - a_1)(x - a_2) \ldots (x - a_n)$. We call E a splitting field for $f(x)$ over F if $E = F(a_1, a_2, \ldots, a_n)$.

Existence Of Splitting Fields: let F be a field and let $f(x)$ be a nonconstant element of $F[x]$. Then there exists a

splitting field E for $f(x)$ over F.

$F(a) \approx F[x]/\langle p(x)\rangle$: let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)$ is isomorphic to $F[x]/\langle p(x)\rangle$. Furthermore, if $\deg p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0$, where $c_0, c_1, \ldots, c_{n-1} \in F$.

$F(a) \approx F(b)$: let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then the fields $F(a)$ and $F(b)$ are isomorphic.

Let F be a field, let $p(x) \in F[x]$ be irreducible over F, and let a be a zero of $p(x)$ in some extension of F. If ϕ is a field isomorphism from F to F' and b is a zero of $\phi(p(x))$ in some extension of F', then there is an isomorphism from $F(a)$ to $F'(b)$ that agrees with ϕ on F and carries a to b.

Extending $\phi : F \to F'$: let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F', then there is an isomorphism from E to E' that agrees with ϕ on F.

Splitting Fields Are Unique: let F be a field and let $f(x) \in F[x]$. Then any 2 splitting fields of $f(x)$ over F are isomorphic.

Derivative: let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ belong to $F[x]$. The derivative of $f(x)$, denoted by $f'(x)$, is the polynomial $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$ in $F[x]$.

Properties Of The Derivative: let $f(x), g(x) \in F[x]$ and let $a \in F$. Then.
1 $(f(x) + g(x))' = f'(x) + g'(x)$.
2 $(af(x))' = af'(x)$.
3 $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$.

Criterion For Multiple Zeros: a polynomial $f(x)$ over a field F has a multiple zero in some extension E if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.

Zeros Of An Irreducible: let $f(x)$ be an irreducible polynomial over a field F. If F has characteristic 0, then $f(x)$ has no multiple zeros. If F has characteristic $p \neq 0$, then $f(x)$ has a multiple zero only if it is of the form $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Perfect Field: a field F is called perfect if F has characteristic 0 or if F has characteristic p and $F^p = \{a^p | a \in F\} = F$.

Finite Fields Are Perfect: every finite field is perfect.

Criterion For No Multiple Zeros: if $f(x)$ is an irreducible polynomial over a perfect field F, then $f(x)$ has no multiple zeros.

Zeros Of An Irreducible Over A Splitting Field: let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$ over F. Then all the zeros of $f(x)$ in E have the same multiplicity.

Factorization Of An Irreducible Over A Splitting Field: let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$. Then $f(x)$ has the form $a(x-a_1)^n(x-a_2)^n \dots (x-a_t)^n$ where $a_1, a_2, \dots, a_t$ are distinct elements of E and $a \in F$.

Types Of Extensions: let E be an extension field of a field F and let $a \in E$. We call a algebraic over F is a is the zero of some nonzero polynomial in $F[x]$. If a is not algebraic over F, it is called transcendental over F. An extension E of F is called an algebraic extension of F if every element of E is algebraic over F. If E is not an algebraic extension of F, it is called a transcendental extension of F. An extension of F of the form $F(a)$ is called a simple extension of F.

Characterization Of Extensions: let E be an extension field of the field F and let $a \in E$. If a is transcendental over F, then $F(a) \approx F(x)$. If a is algebraic over F, then $F(a) \approx F[x]/\langle p(x) \rangle$, where $p(x)$ is a polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F.

Uniqueness Property: if a is algebraic over a field F, then there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(a) = 0$.

Divisibility Property: let a be algebraic over F, and let $p(x)$ be the minimal polynomial for a over F. If $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

Degree Of An Extension: let E be an extension field of a field F. We say that E has degree n over F and write $[E : F] = n$ if E has dimension n as a vector space over F. If $[E : F]$ is finite, E is called a finite extension of F; otherwise, we say that E is an infinite extension of F.

Finite Implies Algebraic: if E is a finite extension of F, then E is an algebraic extension of F.

$[K : F] = [K : E][E : F]$: let K be a finite extension field of the field E and let E be a finite extension field of the field F. Then K is a finite extension field of F and $[K : F] = [K : E][E : F]$.

Primitive Element Theorem: if F is a field of characteristic 0, and a and b are algebraic over F, then there is an element c in $F(a, b)$ such that $F(a, b) = F(c)$.

Algebraic Over Algebraic Is Algebraic: if K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.

Subfield Of Algebraic Elements: let E

be an extension field of the field F. Then the set of all elements of E that are algebraic over F is a subfield of E.

Classification Of Finite Fields: for each prime p and each positive integer n, there is, up to isomorphism, a unique finite field of order p^n.

Structure Of Finite Fields: as a group under addition, $\mathrm{GF}(p^n)$ is isomorphic to $Z_p \oplus Z_p \oplus \cdots \oplus Z_p$. As a group under multiplication, the set of nonzero elements of $\mathrm{GF}(p^n)$ is isomorphic to Z_{p^n-1} (and is, therefore, cyclic).

$[\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$.

$\mathrm{GF}(p^n)$ Contains An Element Of Degree n: let a be a generator of the group of nonzero elements of $\mathrm{GF}(p^n)$ under multiplication. Then a is algebraic over $\mathrm{GF}(p)$ of degree n.

Subfields Of A Finite Field: for each divisor m of n, $\mathrm{GF}(p^n)$ has a unique subfield of order p^m. Moreover, these are the only subfields of $\mathrm{GF}(p^n)$.

Conjugacy Class Of a: let a and b be elements of a group G. We say that a and b are conjugate in G (and call b a conjugate of a) if $xax^{-1} = b$ for some x in G. The conjugacy class of a is the set $\mathrm{cl}(a) = \{xax^{-1} | x \in G\}$.

Number Of Conjugates Of a: let G be a finite group and let a be an element of G. Then, $|\mathrm{cl}(a)| = |G : C(a)|$.

$|\mathrm{cl}(a)|$ Divides $|G|$: in a finite group, $|\mathrm{cl}(a)|$ Divides $|G|$.

Class Equation: for any finite group G, $|G| = \sum |G : C(a)|$ where the sum runs over 1 element a from each conjugacy class of G.

p-Groups Have Nontrivial Centers: let G be a nontrivial finite group whose order is a power of a prime p. Then $Z(G)$ has more than 1 element.

Groups Of Order p^2 Are Abelian: if $|G| = p^2$, where p is prime, then G is Abelian.

Existence Of Subgroups Of Prime-Power Order: let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least 1 subgroup of order p^k.

Sylow p-Subgroup: let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide G, then any subgroup of G of order p^k is called a Sylow p-subgroup of G.

Cauchy's Theorem: let G be a finite group and let p be a prime that divides the order of G. Then G has an element of order p.

Conjugate Subgroups: let H and K be subgroups of a group G. We say that H and K are conjugate in G if there is an element g in G such that $H = gKg^{-1}$.

Sylow's Second Theorem: if H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is

contained in some Sylow p-subgroup of G.

Sylow's Third Theorem: let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G is equal to 1 modulo p and divides m. Furthermore, any 2 Sylow p-subgroups of G are conjugate.

A Unique Sylow p-Subgroup Is Normal: a Sylow p-subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow p-subgroup of G.

Cyclic Groups Of Order pq: if G is a group of order pq, where p and q are primes, $p < q$, and p does not divide $q - 1$, then G is cyclic. In particular, G is isomorphic to Z_{pq}.

Simple Group: a group is simple if its only normal subgroups are the identity subgroup and the group itself.

Sylow Test For Nonsimplicity: let n be a positive integer that is not prime, and let p be a prime divisor of n. If 1 is the only divisor of n that is equal to 1 modulo p, then there does not exist a simple group of order n.

$2 \cdot$ Odd Test: an integer of the form $2 \cdot n$, where n is an odd number greater than 1, is not the order of a simple group.

Generalised Cayley Theorem: let G be a group and let H be a subgroup of G. Let S be the group of all permutations of the left cosets of H in G. Then there is a homomorphism from G into S whose kernel lies in H and contains every normal subgroup of G that is contained in H.

Index Theorem: if G is a finite group and H is a proper subgroup of G such that $|G|$ does not divide $|G : H|!$, then H contains a nontrivial normal subgroup of G. In particular, G is not simple.

Embedding Theorem: if a finite non-Abelian simple group G has a subgroup of index n, then G is isomorphic to a subgroup of A_n.

Equivalence Classes Of Words: for any pair of elements u and v of $W(S)$, we say that u is related to v if v can be obtained from u by a finite sequence of insertions or deletions of words of the form xx^{-1} or $x^{-1}x$, where $x \in S$.

Equivalence Classes Form A Group: let S be a set of distinct symbols. For any word u in $W(S)$, let $\bar{u}$ denote the set of all words in $W(S)$ equivalent to u (that is,$\bar{u}$ is the equivalence class containing u). Then the set of all equivalence classes of elements of $W(S)$ is a group under the operation $\bar{u} \cdot \bar{v} = \bar{uv}$.

Universal Mapping Property: every group is a homomorphic image of a free group.

Universal Factor Group Property: every group is isomorphic to a factor group of

a free group.

Generators And Relations: let G be a group generated by some subset $A = \{a_1, a_2, \ldots, a_n\}$ and let F be the free group on A. Let $W = \{w_1, w_2, \ldots, w_t\}$ be a subset of F and let N be the smallest normal subgroup of F containing W. We say that G is given by the generators $a_1, a_2, \ldots, a_n$ and the relations $w_1 = w_2 = \ldots \ w_t = e$ if there is an isomorphism from F/N onto G that carries $a_i N$ to a_i.

Dyck's Theorem: let $G = \langle a_1, a_2, \ldots, a_n | w_1 = w_2 = \cdots = w_t = e \rangle$ and let $\bar{G} = \langle a_1, a_2, \ldots, a_n | w_1 = w_2 = \cdots = w_{t+k} = e \rangle$. Then $\bar{G}$ is a homomorphic image of G.

Largest Group Satisfying Defining Relations: if K is a group satisfying the defining relations of a finite group G and $|K| \geq |G|$, then K is isomorphic to G.

Classification Of Groups Of Order 8: up to isomorphism, there are only five groups of order $8 : Z_8, Z_4 \oplus Z_2, Z_2 \oplus Z_2 \oplus Z_2, D_4$, and the quaternions.

Characterization Of Dihedral Groups: any group generated by a pair of elements of order 2 is dihedral.

Isometry: an isometry of n-dimensional space $\mathbb{R}^n$ is a function from $\mathbb{R}^n$ onto $\mathbb{R}^n$ that preserves distance.

Symmetry Group Of A Figure In $\mathbb{R}^n$: let F be a set of points in $\mathbb{R}^n$. The symmetry group of F in $\mathbb{R}^n$ is the set of all isometries of $\mathbb{R}^n$ that carry F onto itself. The group operation is function composition.

Finite Symmetry Groups In The Plane: the only finite plane symmetry groups are Z_n and D_n.

Finite Groups Of Rotations In $\mathbb{R}^3$: up to isomorphism, the finite groups of rotations in $\mathbb{R}^3$ are Z_n, D_n, A_4, S_4, A_5.

Elements Fixed By ϕ: for any group G of permutations on a set S and any ϕ in G, we let $\text{fix}(\phi) = \{i \in S | \phi(i) = i\}$. This set is called the elements fixed by ϕ (or more simply, fix of ϕ).

Burnside's Theorem: if G is a finite group of permutations on a set S, then the number of orbits of elements of S under G is $\frac{1}{|G|} \sum_{\phi \in G} |\text{fix}(\phi)|$.

Cayley Digraph Of A Group: let G be a finite group and let S be a set of generators for G. We define a digraph $\text{Cay}(S : G)$, called the Cayley digraph on G with generating set S, as follows.
1 each element of G is a vertex of $\text{Cay}(S : G)$.
2 for $x, y \in G$, there is an arc from x to y if and only if $xs = y$ for some $s \in S$.

A Necessary Condition: $\text{Cay}(\{(1,0),(0,1)\} : Z_m \oplus Z_n)$ does not have a Hamiltonian circuit when m and n are coprime and greater than 1.

A Sufficient Condition: $\text{Cay}(\{(1,0),(0,1)\} : Z_m \oplus Z_n)$ has a Hamiltonian circuit when $n|m$.

Abelian Groups Have Hamiltonian Paths: let G be a finite Abelian group, and let S be any (nonempty) generating set for G. Then $\text{Cay}(S : G)$ has a Hamiltonian path.

Linear Code: an (n, k) linear code over a finite field F is a k-dimensional subspace V of the vector space $F^n = F \oplus F \oplus \cdots \oplus F$ over F. The members of V are called the code words. When F is Z_2, the code is called binary.

Hamming Distance, Hamming Weight: the Hamming distance between 2 vectors in F^n is the number of components in which they differ. The Hamming weight of a vector is the number of nonzero components of the vector. The Hamming weight of a linear code is the minimum weight of any nonzero vector in the code.

Properties Of Hamming Distance And Hamming Weight: for any vectors $u, v, w, d(u, v \leq d(u, w) + d(w, v))$ and $d(u, v) = \text{wt}(u - v)$.

Correcting Capability Of A Linear Code: if the Hamming weight of a linear code is at least $2t + 1$, then the code can correct any t or fewer errors. Alternatively, the same code can detect any $2t$ or fewer errors.

Orthogonality Relation: let C be a systematic (n, k) linear code over F with a standard generator matrix G and parity-check matrix H. Then, for any vector v in F^n, we have $vH = 0$ (the zero vector) if and only if v belongs to C.

Parity-Check Matrix Decoding: Parity-check matrix decoding will correct any single error if and only if the rows of the parity-check matrix are nonzero and no row is a scalar multiple of any other row.

Coset Decoding Is Nearest-Neighbor Decoding: in coset decoding, a received word w is decoded as a code word c such that $d(w, c)$ is a minimum.

Syndrome: if an (n, k) linear code over F has a parity-check matrix H, then, for any vector u in F^n, the vector uH is called the syndrome of u.

Same Coset - Same Syndrome: let C be an (n, k) linear code over F with a parity-check matrix H. Then, 2 vectors of F^n are in the same coset of C if and only if they have the same syndrome.

Automorphism, Galois Group, Fixed Field Of H: let E be an extension field of the field F. An automoprhism of E is a ring isomorphism from E onto E. The Galois group of E over F, $\text{Gal}(E/F)$, is the set of all automorphisms of E that take every element of F to itself. If H is a subgroup of $\text{Gal}(E/F)$, the set $E_H = \{x \in E | \phi(x) = x \text{ for all } \phi \in H\}$ is called the fixed field of H.

Fundamental Theorem Of Galois Theory: let F be a field of characteristic 0 or a finite field. If E is the splitting field over F for some polynomial in $F[x]$, then the mapping from the set of subfields of E containing F to the set of subgroups of $\text{Gal}(E/F)$ given by $K \to \text{Gal}(E/F)$ is a one-to-one correspondence. Furthermore, for any subfield K of E containing F.
1 $[E : K] = |\text{Gal}(E/F)|$ and $[K : F] = |\text{Gal}(E/F)|/|\text{Gal}(E/K)|$. [The index of $\text{Gal}(E/K)$ in $\text{Gal}(E/F)$ equals the degree of K over F].
2 if K is the splitting field of some polynomial in $F[x]$, then $\text{Gal}(E/K)$ is a normal subgroup of $\text{Gal}(E/F)$ and $\text{Gal}(K/F)$ is isomorphic to $\text{Gal}(E/F)/\text{Gal}(E/K)$.
3 $K = E_{\text{Gal}(E/K)}$. [The fixed field of $\text{Gal}(E/K)$ is K]
4 if H is a subgroup of $\text{Gal}(E/F)$, then $H = \text{Gal}(E/E_H)$. [The automorphism group of E fixing E_H is H].

Solvable By Radicals: let F be a field, and let $f(x) \in F[x]$. We say that $f(x)$ is solvable by radicals over F is $f(x)$ splits in some extension $F(a_1, a_2, \ldots, a_n)$ of F and there exist positive integers $k_1, k_2, \ldots, k_n$ such that $a_1^{k_1} \in F$ and $a_i^{k_i} \in F(a_1, a_2, \ldots, a_{i-1})$ for $i = 2, 3, \ldots, n$.

Solvable Group: we say that a group G is solvable if G has a series of subgroups $\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_k = G$, where, for each $0 \leq i < k$, H_i is normal in H_{i+1} and H_{i+1}/H_i is Abelian.

Condition For $\text{Gal}(E/F)$ To Be Solvable: let F be a field of characteristic 0 and let $a \in F$. If E is the splitting field of $x^n - a$ over F, then the Galois group $\text{Gal}(E/F)$ is solvable.

Factor Group Of A Solvable Group Is Solvable: a factor group of a solvable group is solvable.

N And G/N Solvable Implies G Is Solvable: let N be a normal subgroup of a group G. If both N and G/N are solvable, then G is solvable.

Solvable By Radicals Implies Solvable Group: let F be a field of characteristic 0 and let $f(x) \in F[x]$. Suppose that $f(x)$ splits in $F(a_1, a_2, \ldots, a_t)$, where $a_1^{n_1} \in F$ and $a_i^{n_i} \in F(a_1, a_2, \ldots, a_{i-1})$ for $i = 2, 3, \ldots, t$. Let E be the splitting field for $f(x)$ over F in $F(a_1, a_2, \ldots, a_t)$. Then the Galois group $\text{Gal}(E/F)$ is solvable.

Cyclotomic Polynomial: for any positive integer n, let $w_1, w_2, \ldots, w_{\phi(n)}$ denote the primitive nth roots of units. The nth cyclotomic polynomial over $\mathbb{Q}$ is the polynomial $\Phi_n(x) = (x - w_1)(x - w_2)\ldots(x - w_{\phi(n)})$.

$x^n - 1 = \prod_{d|n} \Phi_d(x)$: for every positive integer n, $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where the product runs over all positive divisors d of n.

$\Phi_d(x)$ Has Integer Coefficients: for every positive integer n, $\Phi_d(x)$ has integer coefficients.

$\Phi_d(x)$ Is Irreducible Over $\mathbb{Z}$: the cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.

$\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \approx U(n)$: let w be a primitive nth root of unity. Then $\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \approx U(n)$.

$\mathbb{Q}(\cos(2\pi n)) \subseteq \mathbb{Q}(w)$: let n be a positive integer and let $w = \cos(2\pi/n) + i\sin(2\pi/n)$. Then $\mathbb{Q}(\cos(2\pi n)) \subseteq \mathbb{Q}(w)$.

Constructibility Criteria For A Regular n-Gon: it is possible to construct the regular n-gon with a straightedge and compass if and only if n has the form $2^k p_1 p_2 \dots p_t$, where $k \geq 0$ and the p_is are distinct primes of the form $2^m + 1$

Reflection

I deeply thank the people who taught me and will continue to teach others, young and old, for years to come.

Hans Magnus Enzensberger, George Lenchner, Sam Baethge, Max Warshauer, Jian Shen, David Patrick, Richard Rusczyk, Mathew Crawford, Sandor Lehoczky, Palmer Mebane, Naoki Sato, Valentin Vornicu, Titu Andreescu, Zuming Feng, Po-Shen Loh, Yufei Zhao, Cosmin Pohoata, Pranav Sriram, Evan Chen, Nets Katz, Kiran Kedlaya, Joe Gallian, David Rusin, Inna Zakharevich, Peter Winkler, Alexander Bogomolny, Antti Laaksonen, Colin Hughes, Jeff Erickson, Umesh Vazirani, Robert Tarjan, Donald Knuth, Ronald Graham, Richard Stanley, Zach Wissner-Gross, Oliver Roeder, Ken Ono, Pradeep Mutalik, Gadi Aleksandrowicz, Oded Margalit, James Shearer, Don Coppersmith, Mark Joshi, Timothy Falcon Crack, Paul Wilmott, Xinfeng Zhou, Frederick Mosteller, Dan Stefanica, Marcos Lopez De Prado, Geoffrey Grimmett, David Stirzaker, Gordan Zitkovic, Milica Cudina, Dusan Djukic, Fedor Petrov, Geoff Smith, C J Bradley, and all other composers of tasks, textbooks, puzzles, and source notes.

Meta and habits are powerful; With good praxis, one approaches peak performance.

The lesson of the Art Of Problem Solving books ought to have been that I can contemplate a maths book, solve a sequence of tasks, and learn. I should have continued doing this earlier with an exploration of further texts because I want to solve hard problems and challenge myself each and every day with increasingly complex structure.

I encourage those who score ≈ 21 points on the USAMO to study a healthful quantity of higher maths. Linear algebra, analysis, combinatorics, algebra, algorithms, partial differential equations etc. with .pdf files from Library Genesis. I suggest attempting to solve every task in reasonable time from a text which contains solutions.

Undergraduates and graduate students can pursue living alone in an optimised quiet [33 dB NRR ear plugs] odourless warm home with a comfortable bed, bed desk, and machine. Thus, one can simply wake up, work, focus in peace and calm.